**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

**(51) International Patent Classification 6 :** G07F 7/10

A1

**(11) International Publication Number:** WO 99/40548

**(43) International Publication Date:** 12 August 1999 (12.08.99)

**(21) International Application Number:** PCT/GB99/00289

**(22) International Filing Date:** 28 January 1999 (28.01.99)

**(30) Priority Data:**
60/073,906 6 February 1998 (06.02.98) US

**(71) Applicant:** MONDEX INTERNATIONAL LIMITED [GB/GB]; 1st floor, 47–53 Cannon Street, London EC4M 5SQ (GB).

**(72) Inventors:** PEACHMAN, Anthony, David; 31 Ashdown Avenue, Saltdean, Brighton, East Sussex BN2 8AH (GB). SIMMONS, Ian, Stephen; The Elms, School Road, Broughton, Cambridgeshire PE17 3AT (GB).

**(74) Agent:** REDDIE & GROSE; 16 Theobalds Road, London WC1X 8PL (GB).

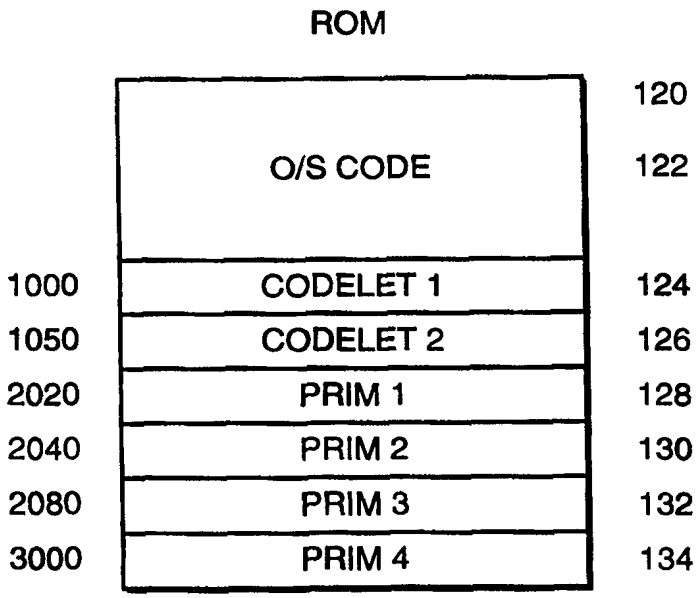
**(81) Designated States:** AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*
*Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

**(54) Title:** CONFIGURATION OF IC CARD

**(57) Abstract**

A secure multiple application card system is provided including an IC card having a microprocessor, a ROM and an EEPROM, wherein program instructions are stored in the ROM at time of manufacture, and at time of personalization, an address table is stored in the EEPROM. Upon operation of the IC card, the operating system calls the program instructions, including codelets and primitives, in accordance with the addresses indicated in the address table.



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **AL** | Albania | **ES** | Spain | **LS** | Lesotho | **SI** | Slovenia |
| **AM** | Armenia | **FI** | Finland | **LT** | Lithuania | **SK** | Slovakia |
| **AT** | Austria | **FR** | France | **LU** | Luxembourg | **SN** | Senegal |
| **AU** | Australia | **GA** | Gabon | **LV** | Latvia | **SZ** | Swaziland |
| **AZ** | Azerbaijan | **GB** | United Kingdom | **MC** | Monaco | **TD** | Chad |
| **BA** | Bosnia and Herzegovina | **GE** | Georgia | **MD** | Republic of Moldova | **TG** | Togo |
| **BB** | Barbados | **GH** | Ghana | **MG** | Madagascar | **TJ** | Tajikistan |
| **BE** | Belgium | **GN** | Guinea | **MK** | The former Yugoslav Republic of Macedonia | **TM** | Turkmenistan |
| **BF** | Burkina Faso | **GR** | Greece | | | **TR** | Turkey |
| **BG** | Bulgaria | **HU** | Hungary | **ML** | Mali | **TT** | Trinidad and Tobago |
| **BJ** | Benin | **IE** | Ireland | **MN** | Mongolia | **UA** | Ukraine |
| **BR** | Brazil | **IL** | Israel | **MR** | Mauritania | **UG** | Uganda |
| **BY** | Belarus | **IS** | Iceland | **MW** | Malawi | **US** | United States of America |
| **CA** | Canada | **IT** | Italy | **MX** | Mexico | **UZ** | Uzbekistan |
| **CF** | Central African Republic | **JP** | Japan | **NE** | Niger | **VN** | Viet Nam |
| **CG** | Congo | **KE** | Kenya | **NL** | Netherlands | **YU** | Yugoslavia |
| **CH** | Switzerland | **KG** | Kyrgyzstan | **NO** | Norway | **ZW** | Zimbabwe |
| **CI** | Côte d'Ivoire | **KP** | Democratic People's Republic of Korea | **NZ** | New Zealand | | |
| **CM** | Cameroon | | | **PL** | Poland | | |
| **CN** | China | **KR** | Republic of Korea | **PT** | Portugal | | |
| **CU** | Cuba | **KZ** | Kazakstan | **RO** | Romania | | |
| **CZ** | Czech Republic | **LC** | Saint Lucia | **RU** | Russian Federation | | |
| **DE** | Germany | **LI** | Liechtenstein | **SD** | Sudan | | |
| **DK** | Denmark | **LK** | Sri Lanka | **SE** | Sweden | | |
| **EE** | Estonia | **LR** | Liberia | **SG** | Singapore | | |

# CONFIGURATION OF IC CARD

of which the following is a

## SPECIFICATION

## PRIORITY APPLICATION

This application claims priority to United States Provisional Application Serial No. 60/073,906 filed on February 6, 1998, entitled "Remote Configuration of IC Card."

## RELATED APPLICATION

This application is related to U.S. Provisional Application Serial No.60/072,561 filed on January 22, 1998 entitled Codelets and U.S. Patent Application Serial No. 09/076,551 filed on May 12, 1998 entitled Secure Multiple Application Card System and Process, which are hereby incorporated by reference, and of which USSN 09/076,551 is included herein as Annex A.

## BACKGROUND OF INVENTION

Integrated circuit cards are becoming increasingly used for many different purposes in the world today. An IC card typically is the size of a conventional credit card on which a computer chip is embedded. It comprises a microprocessor, read-only-memory (ROM), electrically erasable programmable read-only-memory (EEPROM), an Input/Output (I/O) mechanism and other circuitry to support the microprocessor in its operations. An IC card may contain one or more applications in memory. MULTOS™ is a multiple application operating system which runs on IC cards, among other platforms, and allows multiple applications to be executed on the card itself. This allows a card user to run many programs stored in the card (for example, credit/debit, electronic money/purse and/or loyalty applications) irrespective of the type of terminal (i.e., ATM, telephone and/or POS) in which the card is inserted for use.

IC cards typically have limited storage capacity due to the size and cost restraints of locating memory on the card. Applications for multi-application smart cards are written in a programming language and are typically stored in the EEPROM whose contents can be changed during the lifetime of the card. One example of a programming language used in IC cards is the Multos Executable Language (MEL™). The MEL program instructions are read from EEPROM when they are executed and are interpreted by the operating system stored in ROM.

The ROM on the IC card includes the operating system written in assembler language code for the particular integrated circuit configuration (native language type code). The operating system code stored in ROM is fixed when the ROM is initially written and the

information stored in ROM will not change for the life of the card.

Also present in ROM can be subroutines called primitives written in a native language code for the microprocessor which can be called by either the operating system itself or by applications when they are executed. Primitives are written in native language (i.e. assembler language) so that they can be executed very quicky and minimal interpretation of the instructions is necessary for execution. These primitives are collections of instructions which typically perform a desired function, such as a mathematical or cryptographic function. The instructions are never changed during the lifetime of the card. Any data used or accessed by the primitives are stored in EEPROM so that the contents of the data elements can change as necessary.

Also capable of being stored in ROM are "codelets," which are sets of instructions written in a programming language (not native language code). These codelets can be stored in ROM so as to maximize the usage of memory and allow ROM to store complete applications as well as primitives. The codelet can be as small as one instruction or as large as will fit into the remaining ROM memory space. For example, the purse application described above can be stored in ROM when the card is initialized in order to free up space in EEPROM for additional applications which can be loaded at any time.

Once data is stored in ROM, the data can never be modified or deleted and new data cannot be added after ROM is set. Moreover, in prior art systems, when the chip card is manufactured, a primitive address table is stored on the card which allows the operating system to locate the memory address of a primitive. This address table in ROM is also permanently set.

In this system, described in an application copending with this one (see Serial No.

09/076,551, incorporated herein as Annex A), subsequent to card manufacture (at which time the ROM is fixed), the card is "personalized." This personalization step takes place either shortly after the card is made or anytime thereafter, up to a period of months or more. In the meantime, before the card is personalized, cards remain "blank" (i.e., unassigned to an individual user or group) and typically will be held at the card manufacturer or card issuer until needed. During this stage, because the cards have not yet been personalized, there is a greater risk that the cards would be improperly used.

The personalization step -- in which the cards are assigned to a particular user or group -- takes place at a location different from the card manufacturer generally under control of the card-issuer (i.e., the bank issuing the card) or some other personalization bureau ("PB"). A separate and preferably centrally located Certification Authority, which oversees the cards' interaction, provides the usually remote PB with appropriate security data, discussed below, to allow the PB to personalize (i.e., enable) the card, and to allow an application provider to load (either at the time of enablement or later) an application program, such as a purse application, onto the card.

One of the problems confronting multi-application card designers is how to address the situation where after the primitive or codelet is masked or otherwise stored in the ROM at the time of manufacture (and thus cannot thereafter be changed), the primitive or codelet needs to be replaced, modified or updated to fix a bug or to take advantage of a more efficient or effective routine. Another concern is to ensure that the original primitives and codelets masked into ROM are not capable of use until the card is personalized, i.e. enabled for a particular user or

group, with individual keys and identifiers. Accordingly the invention aims to address at least some of the foregoing problems and more particularly to provide a method and system which solves these problems.

## SUMMARY OF THE INVENTION

The applicant here has determined that one way to achieve these aims is by loading in EEPROM at the personalization step and not at the manufacturing step an address table assigning to each primitive and/or codelet a name and corresponding address identifying where the primitive and/or codelet can be found in memory. In this manner, if the primitive masked in ROM at the time of manufacture needs to be changed, only the address for that primitive needs to be changed to point to the location in which the updated primitive sits. In addition, since neither an application nor the operating system will know where the primitive is located without a stored address table, the primitives cannot be called and the card cannot run until the primitive address table is loaded at the personalization step. This prevents use of the card until it is enabled at the personalization step.

## BRIEF DESCRIPTION OF THE DRAWINGS

Further objects, features and advantages of the invention will become apparent from the following detailed description taken in conjunction with the accompanying figures showing illustrative embodiments of the invention, in which

Fig. 1 is a block diagram illustrating the three states in the life of a multi-application IC card in a secure system;

Fig. 2 is a block diagram showing the components of the system architecture for the enablement process of an IC card in a secure multi-application IC card system;

Fig. 3 is a block diagram illustrating the read only memory space segments for an IC card at the time of manufacture in accordance with an embodiment of the present invention;

Fig. 4 is a block diagram illustrating the electrically erasable programmable read-only-memory space segments for an IC card after it has been loaded at the personalization stage in accordance with an embodiment of the present invention;

Fig. 5 is a block diagram illustrating the address table loaded in EEPROM of an IC card at the personalization stage, in accordance with an embodiment of the present invention;

Fig. 6 illustrates an integrated circuit card which can be used in connection with an embodiment of this invention; and

Fig. 7 is a functional block diagram of the integrated circuit shown in Fig. 6.

Throughout the figures, the same reference numerals and characters, unless otherwise stated, are used to denote like features, elements, components or portions of the illustrated embodiments. Moreover, while embodiments of the subject invention will now be described in detail with reference to the figures, it is done so in connection with the illustrative embodiments. It is intended that changes and modifications can be made to the described embodiments without departing from the true scope and spirit of the subject invention as defined by the appended claims.

## DETAILED DESCRIPTION OF THE DRAWINGS

Figure 1 shows the three steps involved in providing an operational multi-application IC card in a secure system. The first step is the card manufacturing step 101. The second step is the personalization step 103 where card personalization data (also called entity authentication data) is loaded onto the card. The third step is the application loading step 105 which checks to see if a card is qualified to receive an application, i.e., when the personalization data is checked against the application permissions data associated with the application to be loaded. Each of these three steps is described in detail in Annex A.

Figure 2 shows the components of the system architecture for the card initialization process of an IC card in a secure multiple application IC card system. The system includes a card manufacturer 102, a personalization bureau 104, an application loader 106, the IC card 107 being initialized, the card user 109 and the certification authority 111 for the entire multiple application secure system. The card user 109 is the person or entity who will use the stored applications on the IC card.

The card user would contact a card issuer 113, such as a bank which distributes IC cards, and request an IC card with the two applications both residing in memory of a single IC card. The integrated circuit chip for the IC card would be manufactured by manufacturer 102 and sent to the card issuer 113 (or an entity acting on its behalf) in the form of an IC chip on a card. During the manufacturing process, data is transmitted 115 via a data conduit from the manufacturer 102 to card 107 and stored in IC card 107's memory. (Any of the data conduits

described in this figure could be a telephone line, Internet connection or any other transmission medium.) The certification authority 111, which maintains encryption/decryption keys for the entire system, transmits 117 security data (i.e., global public key) to the manufacturer over a data conduit which is placed on the card by the manufacturer along with other data, such as the card enablement key and card identifier. The card's multiple application operating system is also stored in ROM and placed on the card by the manufacturer. After the cards have been initially processed, they are sent to the card issuer for personalization and application loading.

The card issuer 113 performs, or has performed by another entity, two separate functions. First, the personalization bureau 104 personalizes the IC card 107 in the ways described above, and second, the application loader 106 loads the application provided the card is qualified, as described in Annex A

Backtracking now to the time of manufacture, the ROM 120 of IC card is loaded, as illustrated in Figure 3, with operating system code 122, codelets 1 and 2 identified respectively as 124, 126, at addresses 1000 and 1050, and primitives 1, 2, 3, 4 identified respectively are 128, 130, 132, 134, at addresses 2020, 2040, 2080, and 3000. The addresses are preferably physical addresses in ROM, an offset from a primitive starting pointer, or any other addressing scheme.

Subsequently, as described above, the card is personalized. The CA provides the PB with personalization information, which may include an individual key set 136. This information is sent to the PB usually at a remote location either through the Internet, by CD ROM or other data conduit or storage device. The PB remotely loads this information onto the

EEPROM of the card (see Fig. 4) along with certain identifiers 138, such as a card identification, an issuer identification, product type identification (representing the type of application, i.e., purse, loyalty, etc.) and the date of loading. Additional primitive or codelet code can also be loaded at this time.

In accordance with an embodiment of this invention, the PB further remotely loads onto the EEPROM of the card the codelet/primitive address table 140. As shown in Fig. 5, this address table 140 contains a listing of the names of the codelets and primitives to be called by either the application program or operating system together with the memory addresses containing the code to be called. The location of code corresponding to a primitive call by the operating system or an application will be determined at this time. Thus, the controlling authority or system operator can select which version of code stored in the card will be executed when a particular primitive name is called.

In this particular case, a program instruction such as:

CALL PRIM 4 (DATA)

would result in a search of the address table to locate the address of PRIM 4. Because a new PRIM 4, with address 3080, was added into the programmable portion of the card memory at time of personalization to replace old PRIM 4, the operating system will simply fetch the new PRIM 4 at location 3080 as indicated in the address table. The old code at memory location 3000 will never be accessed by the operating system because there is no entry in the address table pointing to the old code.

Accordingly, this remote loading of an address table at the time of personalization

allows the system (1) to control enablement until desired; and (2) to make use of a card despite an outdated codelet or primitive which may have been permanently placed in the card at the time of manufacture.

Figure 6 illustrates a card 600 incorporating integrated circuit technology that can be used with the presently claimed invention. Card 600 looks similar to a conventional credit card, but also includes integrated circuit (IC) 622, which contains a microprocessor, and electrical contacts 624 for communication between IC 622 and devices external to card 600. Card 600 can be used for example, as a credit card, a debit card, and\or as an electronic cash card, i.e., a card containing monetary value that can be transferred when the cardholder makes purchases, for example, a MONDEX™ cash card.

Figure 7 is a functional block diagram of the IC section 622 and contains at least processing unit 710 and memory unit 750. Preferably, IC 722 also includes control logic 720, a timer 730, and input/output ports 740. IC section 722 can also include a co-processor 760. Control logic 720 provides, in conjunction with processing unit 710, the control necessary to handle communications between memory unit 750 and input/output ports 740. Timer 730 provides a timing reference signal for processing unit 710 and control logic 720. Co-processor 760 provides the ability to perform complex computations in real time, such as those required by cryptographic algorithms.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise numerous systems and methods which, although not explicitly shown or described herein, embody the principles of the invention and are thus within the spirit and scope of the invention.

The scope of the present disclosure includes any novel feature or combination of features disclosed therein either explicitly or implicitly or any generalisation thereof irrespective of whether or not it relates to the claimed invention or mitigates any or all of the problems addressed by the present invention. The applicant hereby gives notice that new claims may be formulated to such features during the prosecution of this application or of any such further application derived therefrom. In particular, with reference to the appended claims, features from dependent claims may be combined with those of the independent claims and features from respective independent claims may be combined in any appropriate manner and not merely in the specific combinations enumerated in the claims.

ANNEX A TO THE DESCRIPTION

BAKER & BOTTS, L.L.P.
30 ROCKEFELLER PLAZA
NEW YORK, NEW YORK 10112

TO ALL WHOM IT MAY CONCERN:

Be it known that WE, DAVID BARRINGTON EVERETT, STUART JAMES MILLER, ANTHONY DAVID PEACHAM, IAN STEPHENS SIMMONS, TIMOTHY PHILIP RICHARDS and JOHN CHARLES VINER, citizens of GREAT BRITAIN, whose post office addresses are 31 Ashdown Avenue, Saltdean, Brighton, East Sussex BN2 8AH; 9 Woodford Green, The Warren, Bracknell, Berks, RG12 9YQ; 4 Lynwood, Groombridge, Turbridge Wells, Kent, TN3 9LX; The Elms, School Road, Broughton, Cambs, PE17 3AT; 32 Craig Mount, Radlett, Herts, WD7 7LW, and Hydes, Woodlands Lane, Windlesham; respectively, have invented an improvement in

**SECURE MULTIPLE APPLICATION CARD SYSTEM AND PROCESS**

of which the following is a

SPECIFICATION

PRIORITY APPLICATION

This application claims priority to United States Provisional application 60/046,514 filed on May 15,1997, entitled "Design for a Multi Application Smart Card" and United States Provisional application 60/046,543 filed on May 15, 1997, entitled "Virtual Machine for a Multi Application Smart Card", as well as United States application No. 09/023,057 filed on February 12,1998, entitled "Secure Multi-Application IC Card System Having Selective Loading and Deleting Capability", all of which are incorporated herein by reference.

ANNEX A TO THE DESCRIPTION

## BACKGROUND OF INVENTION

Integrated circuit ("IC") cards are becoming increasingly used for many different purposes in the world today. An IC card (also called a smart card) typically is the size of a conventional credit card which contains a computer chip including a microprocessor, read-only-memory (ROM), electrically erasable programmable read-only-memory (EEPROM), an Input/Output (I/O) mechanism and other circuitry to support the microprocessor in its operations. An IC card may contain a single application or may contain multiple independent applications in its memory. MULTOS™ is a multiple application operating system which runs on IC cards, among other platforms, and allows multiple applications to be executed on the card itself. This allows a card user to run many programs stored in the card (for example, credit/debit, electronic money/purse and/or loyalty applications) irrespective of the type of terminal (i.e., ATM, telephone and/or POS) in which the card is inserted for use.

A conventional single application IC card, such as a telephone card or an electronic cash card, is loaded with a single application at its personalization stage. That application, however, cannot be modified or changed after the card is issued even if the modification is desired by the card user or card issuer. Moreover, if a card user wanted a variety of application functions to be performed by IC cards issued to him or her, such as both an electronic purse and a credit/debit function, the card user would be required to carry multiple physical cards on his or her person, which would be quite cumbersome and inconvenient. If an application developer or card user desired two different applications to interact or exchange data with each other, such as a purse application interacting with a frequent flyer loyalty application, the card user would be forced to swap multiple cards in and out of the card-receiving terminal, making the transaction difficult, lengthy and
inconvenient.

Therefore, it is beneficial to store multiple applications on the same IC card. For example, a card user may have both a purse application and a credit/debit application on the same card so that the user could select which type of payment (by electronic cash or credit card) to use to make a purchase. Multiple applications could be provided to an

IC card if sufficient memory exists and an operating system capable of supporting multiple applications is present on the card. Although multiple applications could be pre-selected and placed in the memory of the card during is production stage, it would also be beneficial to have the ability to load and delete applications for card post-production as needed.

The increased flexibility and power of storing multiple applications on a single card create new challenges to be overcome concerning the integrity and security of the information (including application code and associated data) exchanged between the individual card and the application provider as well as within the entire system when loading and deleting applications. It would be beneficial to have the capability of the IC card system to exchange data among cards, card issuers, system operators and application providers securely and to load and delete applications securely at any time from either a terminal or remotely over a telephone line, internet or intranet connection or other data conduit. Because these data transmission lines are not typically secure lines, a number of security and entity-authentication techniques must be implemented to make sure that applications being sent over the transmission lines are only loaded on the intended cards.

As mentioned, it is important -- particularly where there is a continuing wide availability of new applications to the cardholder -- that the system has the capability of adding applications onto the IC card subsequent to issuance. This is necessary to protect the longevity of the IC cards; otherwise, once an application becomes outdated, the card would be useless. In this regard, to protect against the improper or undesired loading of applications onto IC cards, it would be beneficial for the IC card system to have the capability of controlling the loading process and restricting, when necessary or desirable, the use of certain applications to a limited group or number of cards such that the applications are "selectively available" to the IC-cards in the system. This "selective capability" would allow the loading and deleting of applications at, for example, a desired point in time in the card's life cycle. It would also allow the loading of an application only to those cards chosen to receive the selected application.

Accordingly, it is an object of this invention to provide these important features and specifically a secure IC-card system that allows for selective availability of smart card applications which may be loaded onto IC cards.

## SUMMARY OF THE INVENTION

These and other objectives are achieved by the present invention which provides an IC card system comprising at least one integrated circuit card and having a certification authority and a personalisation bureau. The certification authority ("CA") maintains encryption and decryption keys for the entire system and provides the card manufacturer with security data to be placed on the card at manufacture.

Specifically, in a preferred embodiment, an IC card is injected at manufacture with the public key of the CA and a card identifier for uniquely identifying each of the cards. Subsequent to manufacture, the cards are preferably provided to a personalisation bureau ("PB") which could be a card issuer, for enabling the cards. The PB obtains from the cards the identifiers and forwards a list of card identifiers to the CA.

The CA in turn creates a personalisation data block for each card identifier, and each data block preferably includes card personalisation data and an individual key set. The data block is encrypted and forwarded back to the PB. By using the card identifier, the PB then matches the cards with the encrypted data blocks and separately loads each data block onto the matched card, and preferably sets an enablement bit indicating that the card has been enabled and is ready for application loading.

The application loading process is preferably performed at the PB. At first, the system checks to see whether the card to be loaded is qualified (as defined below) to accept the loading of a specific application. The application loader via a terminal will be advised if the card is qualified and, if so, a check will be done using the CA's public key to determine whether the application to be loaded has been signed by the CA's secret key indicating that the application to be loaded has been allowed by the CA.

ANNEX A TO THE DESCRIPTION

## BRIEF DESCRIPTION OF THE DRAWINGS

Further objects, features and advantages of the invention will become apparent from the following detailed description taken in conjunction with the accompanying figures showing illustrative embodiments of the invention, in which

Fig. 1 is block diagram illustrating the three stages in the life of a multi-application IC card in a secure system;

Fig. 2 is a block diagram illustrating the steps of the card manufacture process;

Fig. 3 is a flow diagram illustrating the steps involved in enabling each of the IC cards in the secure system;

Fig. 4 is a block diagram of an IC card chip which can be used in accordance with the invention;

Fig. 5 is a block diagram illustrating the data stored on the IC card as indicated in block 307 of Fig. 3;

Fig. 5A is a schematic of the data structures residing in an IC card and representing personalization data;

Fig. 6 is a flowchart illustrating the steps of loading an application onto an IC card in the secure system;

Fig. 7 is a flow chart illustrating the checking steps as indicated in block 601 of Fig. 6;

Fig. 8 is a flowchart illustrating the steps undertaken in determining if loading of an application may proceed;

Fig. 9 is a block diagram showing the components of the system architecture for the enablement process of an IC card in a secure multi-application IC card system; and

Fig. 10 is a system diagram of entities involved with the use of the IC card once it has been personalized.

ANNEX A TO THE DESCRIPTION

Throughout the figures, the same reference numerals and characters, unless otherwise stated, are used to denote like features, elements, components or portions of the illustrated embodiments. Moreover, while the subject invention will now be described in detail with reference to the figures, it is done so in connection with the illustrative embodiments. It is intended that changes and modifications can be made to the described embodiments without departing from the true scope and spirit of the subject invention as defined by the appended claims.

## DETAILED DESCRIPTION OF THE INVENTION

The present invention provides an IC card system and process which allow the flexibility to load and delete selected applications over the lifetime of a multi-application IC card in response to the needs or desires of the card user, card issuers and/or application developers. A card user who has such a card can selectively load and delete applications as desired if allowed by the card issuer in conjunction with the system operator or Certification Authority ("CA) which controls the loading and deleting process by certifying the transfer of information relating to the process.

By allowing applications to be selectively loaded and deleted from the card, a card issuer can extend additional functionality to an individual IC card without having to issue new cards. Moreover, application developers can replace old applications with new enhanced versions, and applications residing on the same card using a common multiple application operating system may interact and exchange data in a safe and secure manner. For example, a frequent flyer loyalty program may automatically credit one frequent flyer mile to a card user's internal account for every dollar spent with the Mondex purse or with a credit/debit application. By allowing the ability to selectively load and delete applications, the card user, subject to the requirements of the card issuer, also has the option of changing loyalty programs as desired.

A card issuer or application developer may intend that a particular application be loaded on only one card for a particular card user in a card system. A regional bank may desire to have a proprietary application reside only on the cards which the bank issues. The present invention would allow for this selective loading and

specifically allow for the prevention of loading proprietary applications onto unauthorized cards issued by others.

To achieve these desired objectives, the present invention gives each card a specific identity by storing "card personalization data" on the card. Moreover, each application to be loaded or deleted on one or more cards in the system is assigned "application permissions data" which specify the cards upon which the applications may be loaded.

The type of personalized data can vary depending upon the needs and requirements of the card system. In the preferred embodiment, described in greater detail below, the personalization data include unique card identification designation data, the card issuer, the product class or type (which is defined by the card issuer) and the date of personalization. However, not all of these data elements are required to be used and additional elements could also be included.

The application permissions data associated with an application, also described in greater detail below, can be a single value in an identity field or could include multiple values in the identity field. For example, the application permissions data in the card issuer field could represent both product class A and product class B from a certain Bank X, indicating that the application could be loaded onto cards designated as product classes A and B issued by Bank X (as indicated in the card product ID field of the card's personalization data).

In addition, a "global value" could be stored in the issuer field (or other field) of the application permissions data indicating that all IC cards in the system regardless of who issued the card would match this permissions field. In this case, for example, a data value of zero stored in the application permissions card-issuer field will match all of the cards' personalization card-issuer fields.

Figure 1 shows the three steps involved in providing an operational multi-application IC card in a secure system. The first step is the card manufacturing step 101. The second step is the personalization step 103 where card personalization data (also called entity authentication data) is loaded onto the card. The third step is the application loading step 105 which checks to see if a card is qualified to receive an application, i.e., when the personalization data is checked against the application

permissions data associated with the application to be loaded. Each of these three steps is described in detail below.

Card Manufacture

Figure 2 shows the steps necessary in manufacturing an IC card in a secure system. Step 201 manufactures the physical IC card by creating the integrated circuit on silicon and placing it on the card. The integrated circuit chip will include RAM, ROM and EEPROM memories. When the card is first manufactured, a global public key of the system operator (in this case called the Certification Authority (CA)) is stored on each card in ROM in step 203. This will allow the card to authenticate that the source of any message to it is from the CA since the public key on the card will be matched to the CA's secret key.

More specifically, this public key stored on the card will allow the individual card to verify data signed with the CA's private key. The public key of the CA, which is stored on the card, is used only for determining if the data sent to the card was signed with the proper CA private key. This allows the card to verify the source of any message coming from the CA.

Step 205 inserts a card enablement key in a secure portion of EEPROM in the card to facilitate card specific confidentiality during enablement, and step 207 inserts a card identifier in EEPROM of the card. The identifier, which can be accessed by any terminal, will allow the system to determine the identity of the card in later processes. The identifier is freely available and will not be used to authenticate messages.

Step 209 stores the operating system code in ROM on the card including any primitives which are called or supported by the operating system. The primitives are written in native language code (e.g., assembly language) and are stored in ROM. The primitives are subroutines which may be called by the operating system or by applications residing on the card such as mathematic functions (multiply or divide), data retrieval, data manipulation or cryptographic algorithms. The primitives can be executed very quickly because they are written in the native language of the processor.

After the IC cards are manufactured, they are sent to a personalization bureau ("PB") to enable and personalize the card by storing card personalization data in the memory of the card. The terms enablement and personalization are used interchangeably herein to indicate the preparatory steps taken to allow the card to be loaded securely with an application. The individual cards are preferably manufactured in batches and are sent to a personalisation bureau in a group for processing.

Card Enablement/Personalization

Figure 3 shows the steps of the card enablement process when the card arrives at a personalization bureau. The personalization bureau may be the card issuer (e.g., a bank or other financial institution) or may be a third party that performs the service for the card issuer. The personalisation bureau configures the card to a specific user or user class.

Figure 3 specifically shows the steps taken to enable and personalize each IC card which will work within the system. The cards can be placed in a terminal which communicates with IC cards and which reads the card identifier data (previously placed on the card during the manufacturing process - see step 207). This card identification data is read from the card in step 301. The terminal will effectively send a "get identification data" command to the card and the card will return the identification data to the terminal.

The PB typically processes a group of cards at the same time, and will first compile a list of IC card identification data for the group of cards it is personalizing. The PB then sends electronically (or otherwise) this list of identification data to the Certification Authority ("CA") which creates a personalisation (or enablement) data block for each card identifier. The data block includes the card personalization data organized in a number of identity fields and an individual key set for the card, discussed below. These data blocks are then encrypted and sent to the PB in step 302. By using the card identification data, the PB then matches the cards with the encrypted data blocks and separately loads each data block onto the matched card. To insure that the CA controls the identity of the card and the integrity of the system, the PB never obtains

knowledge of the content of the data blocks transferred. Some aspects of the personalization are requested by the card issuer to the CA in order to affect their preferred management of the cards they issue. The following additional steps are performed.

Step 303 first checks to see if an enablement bit stored in EEPROM of the card has been already set. If it already has been set, the card has already been configured and personalized and the enablement process will end as shown in step 304. A card cannot be enabled and personalized twice. If the bit has not been set, then the process continues with step 305.

In step 305, the individualized card key set for the card being enabled (which key set is generated at the CA) is stored on the card. The keys can be used later in off-card verification (i.e., to verify that the card is an authentic card). This verification is necessary to further authenticate the card as the one for which the application was intended.

Step 307 generates four different MULTOS Security Manager (MSM) characteristic data elements (otherwise referred to herein as personalization data) for the card at the CA which are used for securely and correctly loading and deleting applications from a particular card. The MSM characteristics also allow for the loading of applications on specific classes of identified cards. (These MSM characteristics are further described in connection with Figure 5.)

Other data can also be stored on the card at this time as needed by the system design such as an address table or further subroutines.

Step 311 sets the enablement bit in EEPROM of the card which indicates that the enablement process has been completed for the particular card. When this bit is set, another enablement process cannot occur on the card. This ensures that only one personalization and enablement process will occur to the card thus preventing illegal tampering of the card or altering the card by mistake. In the preferred embodiment, the enablement bit is initially not set when the card is manufactured and is set at the end of the enablement process.

Figure 4 shows an example of a block diagram of an IC card chip which has been manufactured and personalized. The IC card chip is located on an IC card for use.

ANNEX A TO THE DESCRIPTION

The IC card preferably includes a central processing unit 401, a RAM 403, a EEPROM 405, a ROM 407, a timer 409, control logic 411, an I/O ports 413 and security circuitry 415, which are connected together by a conventional data bus.

Control logic 411 in memory cards provides sufficient sequencing and switching to handle read-write access to the card's memory through the input/output ports. CPU 401 with its control logic can perform calculations, access memory locations, modify memory contents, and manage input/output ports. Some cards have a coprocessor for handling complex computations like cryptographic algorithms. Input/output ports 413 are used under the control of a CPU and control logic alone, for communications between the card and a card acceptance device. Timer 409 (which generates or provides a clock pulse) drives the control logic 411 and CPU 401 through the sequence of steps that accomplish memory access, memory reading or writing, processing, and data communication. A timer may be used to provide application features such as call duration. Security circuitry 415 includes fusible links that connect the input/output lines to internal circuitry as required for testing during manufacture, but which are destroyed ("blown") upon completion of testing to prevent later access. The personalisation data to qualify the card is stored in a secured location of EEPROM 405. The comparing of the personalisation data to applications permissions data is performed by the CPU 401.

Figure 5 shows the steps of generating and loading the four elements of the card personalization data into the memory of the IC cards, and Fig. 5A shows a schematic of bit maps for each identity field residing in the memory of an IC card containing personalisation data in accordance with the present invention. Each data structure for each identity field has its own descriptor code. Step 501 loads the data structure for the identity field "card ID" called "msm_mcd_permissions_mcd_no." This nomenclature stands for MULTOS system manager _ MULTOS card device_ permissions_MULTOS card device number. Although this number is typically 8 bytes long as shown in Fig. 5A, the data could be any length that indicates a unique number for the card. In the preferred embodiment, 2 bytes are dedicated as a signal indicator, 2 bytes comprise a MULTOS Injection Security Module ID (MISM ID) indicating which security module injected the card with its injected keys when it was manufactured, and 4

bytes comprise an Integrated Circuit Card (ICC) serial number which identifies the individual card produced at the particular MISM.

Step 503 loads the data structure for the identity field "issuer ID" called "msm_mcd_permissions_mcd_issuer_id". This nomenclature stands for a MULTOS card device issuer identification number. Each card issuer (such as a particular bank, financial institution or other company involved with an application) will be assigned a unique number in the card system. Each IC card in the MULTOS system will contain information regarding the card issuer which personalized the card or is responsible for the card. A card issuer will order a certain number of cards from a manufacturer and perform or have performed the personalisation process as described herein. For example, a regional bank may order 5,000 cards to be distributed to its customers. The "mcd_issuer_id" data structure on these cards will indicate which issuer issued the cards. In the preferred embodiment, the data structure is 4 bytes long (as shown in Fig. 5A at 503A) to allow for many different issuers in the system although the length of the data structure can vary with the needs of the card system.

Step 505 loads the data structure for the identity field "product ID" called "msm_mcd_permissions_mcd_issuer product_id." This nomenclature stands for MULTOS card device issuer product identification number. Each card issuer may have different classes of products or cards which it may want to differentiate. For example, a bank could issue a regular credit card with one product ID, a gold credit card with another product ID and a platinum card with still another product ID. The card issuer may wish to load certain applications onto only one class of credit cards. A gold credit card user who pays an annual fee may be entitled to a greater variety of applications than a regular credit card user who pays no annual fee. The product ID field identifies the card as a particular class and will later allow the card issuer to check the product ID and only load applications onto cards which match the desired class.

Another way to differentiate products is by application type, such as by categorizing the application as financial, legal, medical and/or recreational, or by assigning particular applications to a group of cards. For example, one card issuer may have different loyalty programs available with different companies to different sets of card users. For example, a bank may have an American Airlines(R) loyalty program and

a British Airways(R) loyalty program for different regions of the country dependent on where the airlines fly. The product type allows the issuer to fix the product classification of the card during the personalization process. When loading applications onto the card, the product type identification number on each card will be checked to make sure it matches the type of card onto which the issuer desires to load. The product type data structure is preferably an indexing mechanism (unlike the other personalisation data structure) of 8 bits (as shown at 505A in Fig. 5A) but could be any length depending upon the needs of the card system. In the illustrated embodiment, the resulting instruction would be to locate the second bit (since the byte's indicated value is 2) in the array to be searched (see discussion of step 809 below).

Step 507 loads the data structure for the identity field data called "msm_mcd_permissions_mcd_controls_data_date." This nomenclature stands for the MULTOS card device controls data date or, in other words, the date on which the card was personalized so that, for example, the application loader can load cards dated only after a certain date, load cards before a certain date (e.g., for application updates) or load cards with a particular data date. The information can include the year, month and day of personalization or may include less information, if desired. The data date data structure is preferably 1 byte in length (see 507A in Fig. 5A) although it could be any length depending upon the needs of the particular card system used.

Once all of the personalisation data structures are loaded and stored in the card, the card has been identified by issuer, product class, date and identification number (and other data fields, if desired), and the card cannot change its identity; these fields cannot be changed in the memory of the card. If a card user wants to change the product-id stored in the card to gain access to different applications available to another product type, a new card will have to be issued to the user containing the correct personalization data. This system is consistent with a gold card member receiving a new card when the classification is changed to platinum.

After the card has been enabled and personalized by storing its individual card key set, MSM personalization characteristics and enablement bit as described in Fig. 3, the card is ready to have applications loaded into its memory.

ANNEX A TO THE DESCRIPTION

Loading Applications

The application loading process contains a number of security and card configuration checks to ensure the secure and proper loading of an application onto the intended IC card. The application loading process is preferably performed at the personalization bureau so that the card will contain one or more applications when the card is issued. The card may contain certain common applications which will be present on every card the issuer sends out, such as an electronic purse application or a credit/debit application. Alternatively, the personalization bureau could send the enabled cards to a third party for the process of loading applications. The multiple application operating system stored in the ROM of each card and the card MSM personalization data is designed to allow future loading and deleting of applications after the card has been issued depending upon the desires of the particular card user and the responsible card issuer. Thus, an older version of an application stored on the IC card could be replaced with a new version of the application. An additional loyalty application could also be added to the card after it has been initially sent to the card user because the application is newly available or the user desires to use the new application. These loading and deleting functions for applications can be performed directly by a terminal or may be performed over telephone lines, data lines, a network such as the Internet or any other way of transmitting data between two entities. In the present IC card system, the process of transmitting the application program and data ensures that only IC cards containing the proper personalization data and which fit on application permissions profile will be qualified and receive the corresponding application program and data.

Figure 6 shows the preferred steps performed in loading an application onto an IC card in the MULTOS IC card system. For this example, the personalization bureau is loading an application from a terminal which enabled the same card. Step 601 performs an "open command" initiated by the terminal which previews the card to make sure the card is qualified to accept the loading of a specific application. The open command provides the card with the application's permissions data, the application's size, and instructs the card to determine (1) if the enablement bit is set indicating the card has been personalized; (2) whether the application code and associated data will fit

in the existing memory space on the card; and (3) whether the personalization data assigned to the application to be loaded allows for the loading of the application onto the particular card at issue. The open command could also make additional checks as required by the card system. These checking steps during the open command execution will be described in detail in conjunction with Figure 7.

After the open command has been executed, the application loader via the terminal will be advised if the card contains the proper identification personalization data and if enough room exists in the memory of the card for the application code and related data. If there is insufficient memory, then a negative response is returned by the card and the process is abended (abnormally ended). If the identification personalization data does not match the applications permissions data, a warning response is given in step 603, but the process continues to the load and create steps. Alternatively, if there is no match, the process may automatically be abended. If a positive response is returned by the card to the terminal in step 605, the application loader preferably proceeds to next steps. The open command allows the application to preview the card before starting any transfer of the code and data.

Step 607 then loads the application code and data onto the IC card into EEPROM. The actual loading occurs in conjunction with create step 609 which completes the loading process and enables the application to execute on the IC card after it is loaded. The combination of the open, load and create commands are sent by the terminal, or another application provider source, to the IC card to perform the application loading process. The operating system in the IC cards is programmed to perform a specific set of instructions with respect to each of these commands so that the IC card will communicate with and properly carry out the instructions from the terminal.

Step 609 performs the create command which at least: (1) checks if an application load certificate is signed (encrypted) by the CA and therefore authenticates the application as a proper application for the system; and (2) checks the card personalization data stored on the card against the permissions profile for the application to be loaded to qualify the card for loading. It may do other checks as required. If one of the checks fails, then a failure response 610 is given and the process aborts. The application after it has passed these checks will be loaded into the memory of the card.

ANNEX A TO THE DESCRIPTION

Figure 7 shows the various steps of the open step 601 of Fig. 6 in more detail. Step 701 determines if the enablement (i.e., control) bit is set. This bit is set when the card has completed its personalization process and has been assigned its personalization data. An application can be loaded on an IC card in the card system only if the card contains the personalization data. If the enablement bit is not set, the card has not been personalized and therefore the card returns a negative response 703 to the terminal. If the enablement bit is set, then the card has been enabled and the test conditions continue with step 711.

Step 711 checks if there is sufficient space in the memory on the card to store the application code and its associated data. Applications will typically have associated data related to their functions. This data will be used and manipulated when the application is run. Storage space in the memory of an IC card is a continuing concern due to the relatively large physical space required for EEPROM and how it fits in the integrated circuit which is desired to be small enough to fit on a credit card sized card. An example of the size of a preset EEPROM on an IC card is 16K bytes although the actual size varies. Applications can range from 1K byte or less for a very simple application up to the size of available memory for a more sophisticated application. The data associated with an application can range from no data being stored in the card memory to a size constrained by the amount of available memory. These varied sizes of application code and data continually increase as applications become more advanced and diverse.

MULTOS as an operating system is not limited by the number of applications and associated data it can store on the card. Thus, if five applications can fit in the available memory of the card, the card user will have greatly increased functionality than if one or two applications were stored on the card. Once a card's memory is filled to its capacity, however, a new application cannot be loaded onto the card unless another application including its code and data of sufficient size can be deleted. Therefore, checking the amount of available space on the card is an important step. If there is not sufficient space, then an insufficient space response 713 will be returned to the terminal. The application loader can then decide if another existing application on the card should be deleted to make room for the new application.

Deletion depends upon the card issuer having an application delete certificate from the CA. If there is sufficient space on the card, then the process continues with step 715.

An example of the testing of memory spaces in step 711 is now described. The numbers used in this example in no way limit the scope of the invention but are used only to illustrate memory space requirements. An IC card may have 16K available EEPROM when it is first manufactured. The operating system data necessary for the operating system may take up 2K of memory space. Thus, 14K would remain. An electronic purse application's code is stored in EEPROM and may take up 8K of memory space. The purse application's required data may take up an additional 4K of memory space in EEPROM. The memory space which is free for other applications would thus be 2K (16K-2K-8K-4K=2K). If a card issuer wants to load a credit/debit application whose code is 6K bytes in size onto the card in this example, the application will not fit in the memory of the IC card. Therefore, the application cannot load the new application without first removing the purse application from the card. If a new credit/debit application was loaded into EEPROM of the IC card, then it would have to overwrite other application's code or data. The application loader is prevented from doing this.

Figure 8 shows the steps performed in determining whether the card's personalization data falls within the permissible set of cards onto which the application at issue may be loaded. These steps are preferably performed during the execution of the "create" command. However, these steps may be performed at any time during the loading or deleting of an application. As described previously, the card is personalized by storing data specific to the card (MSM personalization data) including: a card ID designation specific to an individual card, the card issuer number indicating the issuer of the card, the product type of the card, such as a gold or platinum card, and the date the card was personalized. This data uniquely identifies the card apart from all other IC cards in the system.

Accordingly, applications can be selectively stored on individual cards in the IC card system on virtually any basis, including the following. An application can be loaded selectively to cards containing one or more specific card numbers. An application can be selectively loaded on one or more cards containing a specified card issuer ID. Moreover, an application can be loaded only upon one type of product

specified by the particular card issuer, and/or the application can be loaded only on cards which have a specified date or series of dates of personalization. Each of the personalization data allows an application to be selectively loaded onto certain cards or groups of cards and also ensures that cards without the proper permissions will not receive the application. Personalization data types in addition to the four described can also be used as needed.

The selection of IC cards upon which a particular application may be loaded is made possible by the use of "applications permissions data" which is assigned to the application and represents at least one set of cards upon which the application may be loaded. The set may be based-on virtually any factor, including one or more of the following: card numbers, card issuers, product types or personalization dates. Although the individual card's personalization data typically identify one specific number, one card issuer, one product type and one date, the application's permissions data may indicate a card number or a blanket permission, a card issuer or a blanket permission, and a number of product types and dates.

For example, a frequent loyalty program may be configured to allow its loading and use on cards in different product classes belonging to one card issuer. In addition, the application permissions data may indicate that the loyalty program can be used on gold and platinum product types if the card was issued after May, 1998. Thus, the MSM permissions check will determine if the card's individual personalization data is included in the allowed or permissible set of cards upon which the application may be loaded. If it is, the application will be loaded.

To expedite the comparison process, an alternative embodiment may include setting one or more permissions data at zero representing a blanket permission for that particular data. For instance, by placing a zero for the "card number" entry in the application permissions data or some other value indicating that all cards may be loaded regardless of their number, the system knows not to deny any cards based on their card number. Moreover, if a zero is placed in the application's permissions data "issuer ID," then all cards similarly will pass the "issuer" test comparison. This feature allows greater flexibility in selecting groups of cards. The zero indicator could also be used for other permissions data, as required.

ANNEX A TO THE DESCRIPTION

Referring to Figure 8, each of the permissions data is checked in the order shown, but other orders could be followed because if any one of the permissions fails, the application will be prevented from being loaded on the IC card being checked. The permissions are preferably checked in the order shown. Step 801 checks if the application permissions product type set encompasses the card's product type number stored in the memory of the card. Each card product type is assigned a number by the system operator. The product types are specified for each card issuer because different card issuers will have different product types. The cards are selectively checked to ensure that applications are loaded only on cards of authorized product type. The application permissions product type set can be 32 bytes long which includes multiple acceptable product types or can be a different length depending upon the needs of the system. Using data structure 505A as an example, the operating system would check bit number 2 in the 256 bit array (32 bytes x 8 bits per byte) resulting from the 32 byte long application permissions data structure. If the permissions check fails, then the card returns a failure message to the terminal in step 803. If the product type check passes (for example, the value of bit No. 2 being 1), then the process continues with step 805.

Step 805 checks if the application permissions allowable card issuer number set encompasses the card's issuer number stored in the memory of the card or if the application permissions issuer data is zero (indicating all cards pass this individual permissions check). Each card issuer is assigned a number by the system operator and the cards are selectively checked to ensure that applications are loaded only on cards distributed by authorized card issuers. The application permissions card issuer number set can be 4 bytes long if one issuer is designated or can be longer depending upon the needs of the system. If the issuer check fails, then the card returns a failure message to the terminal in step 807. If the check passes, then the process continues with step 809.

Step 809 checks if the application permissions date set encompasses the card's data date stored in the memory of the card. The date that the IC card was personalised will be stored and will preferably include at least the month and year. The cards are selectively checked to ensure that applications are loaded only on cards with the authorized personalization date. The application permissions date set can be 32 bytes long which includes multiple dates or can be a different length depending upon the needs

of the system. If the date permissions check fails, then the card returns a failure message to the terminal in step 811. If the date check passes, then the process continues with step 813.

Step 813 checks if the application permissions allowable card number set encompasses the card's ID number stored in the card memory or if the application permissions allowable card number data is zero (indicating all cards pass this individual permissions check). The testing of the permissions is performed on the card during the execution of the open, load and create commands. The application permissions card number data set can be 8 bytes long if one number is designated or can be longer depending upon the needs of the system. If the card number check fails, then the card returns a failure message to the terminal in step 815. If the check passes, then the process continues with step 817.

Summary of IC Card System's Process

Figure 9 shows the components of the system architecture for the card initialization process of an IC card in a secure multiple application IC card system. The system includes a card manufacturer 102, a personalization bureau 104, an application loader 106, the IC card 107 being initialized, the card user 109 and the certification authority 111 for the entire multiple application secure system. The card user 131 is the person or entity who will use the stored applications on the IC card. For example, a card user may prefer an IC card that contains both an electronic purse containing electronic cash (such as MONDEX™ and a credit/debit application (such as the MasterCard (R) EMV application) on the same IC card. The following is a description of one way in which the card user would obtain an IC card containing the desired in a secure manner.

The card user would contact a card issuer 113, such as a bank which distributes IC cards, and request an IC card with the two applications both residing in memory of a single IC card. The integrated circuit chip for the IC card would be manufactured by manufacturer 102 and sent to the card issuer 113 (or an entity acting on its behalf) in the form of an IC chip on a card. As discussed above (see steps 201-209), during the manufacturing process, data is transmitted 115 via a data conduit from the

manufacturer 102 to card 107 and stored in IC card 107's memory. (Any of the data conduits described in this figure could be a telephone line, Internet connection or any other transmission medium.) The certification authority 111, which maintains encryption/decryption keys for the entire system, transmits 117 security data (i.e., global public key) to the manufacturer over a data conduit which is placed on the card by the manufacturer along with other data, such as the card enablement key and card identifier. The card's multiple application operating system is also stored in ROM and placed on the card by the manufacturer. After the cards have been initially processed, they are sent to the card issuer for personalization and application loading.

The card issuer 113 performs, or has performed by another entity, two separate functions. First, the personalization bureau 104 personalizes the IC card 107 in the ways described above, and second, the application loader 106 loads the application provided the card is qualified, as described.

Regarding personalization, an individualized card key set is generated by the CA and stored on the card (see Fig. 3). The card is further given a specific identity using MSM personalization (see Fig. 3, step 307 and Fig. 5) including a card ID number, an issuer ID number identifying the card issuer which processed the card, a card product type number which is specified by the card issuer and the date upon which the personalization took place. After the card has been personalized, applications need to be loaded onto the card so that the card can perform desired functions.

The application loader 106, which could use the same terminal or data conduit as personalization bureau 104, first needs to have determined if the card is qualified to accept the application. This comparison process takes place on the card itself (as instructed by its operating system) using the permissions information. The card, if it is qualified, thus selectively loads the application onto itself based upon the card's identity and the card issuer's instructions. The application loader communicates 119 with the IC card via a terminal or by some other data conduit. After the applications have been loaded on the card, the card is delivered to the card user 109 for use.

The secure multiple application IC card system described herein allows for selective loading and deleting of applications at any point in the life cycle of the IC card

after the card has been personalized. Thus, a card user could also receive a personalized card with no applications and then select a desired application over a common transmission line such as a telephone line or Internet connection.

Figure 10 is a system diagram of entities involved with the use of an IC card once it has been personalized. The system includes an IC card 151, a terminal 153, an application load/delete entity 155, the certification authority 157, a card issuer 171 and other IC cards 159 in the system. The arrows indicate communication between the respective entities. The CA 157 facilitates loading and deleting of applications. After providing the MSM permissions data and card specific keyset to the card during card enablements, the CA allows applications to be later loaded and deleted preferably by issuing an application certificate. Application specific keys are required to authenticate communication between a card and terminal. The IC card 151 also can communicate with other IC cards 159. Card issuer 171 is involved with all decisions of loading and deleting applications for a card which it issued. All communications are authenticated and transmitted securely in the system.

For instance, IC card 151 will use the following procedure to load a new application onto the card. IC card 101 is connected to terminal 153 and the terminal requests that an application be loaded. Terminal 153 contacts application load/delete entity 155 which, as a result and in conjunction with card issuer 171, sends the application code, data and application permissions data (along with any other necessary data) to terminal 153. Terminal 153 then queries card 151 to ensure it is the correct card onto which the application may be loaded. If IC card passes the checks discussed above, the application is loaded onto card 151. The CA 157 provides the application load or delete certificate that enables the application to be loaded or deleted from the card. This example shows one way to load the application, but other variations using the same principles could be performed, such as directly loading the application at the application load/delete entity 155.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise numerous systems and methods which, although not explicitly shown or described herein, embody the principles of the invention and are thus within the spirit and scope of the invention.

For example, it will be appreciated that the MSM personalization and permissions data may not only be used for loading applications onto IC cards but also for deleting applications from said cards. The same checks involving MSM permissions and loading applications are made for deleting applications. A delete certificate from the CA authorizing the deletion of an application will control from which cards the application may be deleted. This is accomplished through the personalization data stored on each IC card and the permissions check as described herein.

Moreover, the data may also be applicable to personal computers or other units onto which applications may be loaded which are not physically loaded on cards. In addition, the application's permissions data may actually include data representative of a set or sets to be excluded, instead of included - cards that cannot be loaded with the application.

ANNEX A TO THE DESCRIPTION

WE CLAIM:

1. A secure multiple application card system comprising:

a certification authority for which a public and private key pair are generated;

at least one integrated circuit card including at manufacture said public key of said certification authority and a card identifier for uniquely identifying each said card;

means for creating at said certification authority a personalization data block for at least one card identifier, means for encrypting said personalization data block and forwarding said encrypted data block to a personalization bureau;

means for loading at said personalization bureau said encrypted data block on said card having the card identifier matching said encrypted personalization data block;

means for determining based at least on said encrypted personalization data block whether one of said integrated circuit cards is qualified to accept the loading of a specific application;

means for authenticating said application for loading onto said card by using said public key of said certification authority; and loading means responsive to said determining and authenticating means for securely loading said application onto said card.

2. The system of claim 1, further comprising personalization means for enabling at least one of said cards at said personalization bureau.

3. The system of claim 1, wherein said at least one integrated circuit card further comprises memory means for storing an operating system for instructing said determining means, authentication means and said loading means.

4. The system of claim 2 wherein said at least one integrated circuit card further comprises a card enablement key for facilitating card specific confidentiality.

5. The system of claim 4 wherein said personalization means comprises means for compiling a list of said card identifiers and means for forwarding said list to said authority.

6. The system of claim 5 wherein said personalization data block comprises card personalization data and an individual key set.

7. The system of claim 6 further including means for checking whether said card enablement key has been set, and wherein said means for loading said encrypted data block only loads said block in the event said enablement key has not been set, and wherein said card enablement key is set upon loading said encrypted data block.

8. A secure multiple application card system comprising:

one or more integrated circuit cards each including at manufacture a public key for authenticating the source of any message to it from an authority holding a corresponding secret key, a card enablement key for facilitating card specific confidentiality, a card identifier for uniquely identifying each card, and memory storing an operating system;

personalization means for enabling said card at a personalization bureau, said personalization means including means for compiling a list of said card identifiers and means for forwarding said list to said authority;

means for creating at said authority a personalization data block for each card identifier forwarded to said authority, said data block including card personalization data and an individual key set for each of said cards;

means for encrypting each of said data blocks and means for forwarding said encrypted data blocks to said personalization bureau;

means for checking whether said card enablement key has been set and, if not, for matching said card identifiers with said encrypted data blocks, loading said encrypted data block on its matched corresponding card, and setting said enablement key;

means for determining whether said card is qualified to accept the loading of a specific application; checking means for authenticating said specific application to be loaded by checking whether said application has been signed by said authority; and

means responsive to said determining and checking means for loading said one or more specific applications.

9. A method for securely loading one or more applications on an integrated circuit card comprising the steps of:

transmitting security data including a public key of a certification authority onto an integrated circuit card;

creating at said certification authority a personalization data block for said card, encrypting said data block and forwarding said encrypted data block to a personalization bureau;

loading said encrypted data block onto said card;

determining based at least on said encrypted data block whether said card is qualified to accept the loading of a specific application;

authenticating said application for loading onto said card by using said public key;

loading said application in the event said card is qualified and said application is authenticated.

10. A method for securely deleting one or more applications from an integrated circuit card comprising the steps of:

transmitting security data including a public key of a certification authority onto an integrated circuit card;

creating at said certification authority a personalization data block for said card, encrypting said data block and forwarding said encrypted data block to a personalization bureau;

loading said encrypted data block onto said card;

determining based at least on said encrypted data block whether said card is qualified to accept the deleting of a specific application; deleting said application in the event said card is qualified.

ANNEX A TO THE DESCRIPTION

## ABSTRACT OF THE DISCLOSURE

A secure multiple application card system and process is provided having secure loading and deleting capability by use of a Certification Authority and Personalization Bureau. The certification authority maintains the security of the system by requiring IC cards to be injected with its public key and a card identifier for uniquely identifying each card, by providing a personalization data block for each card, and by signing with its private key all applications to be loaded or deleted from the IC card.

CLAIMS

1. A secure multiple application card system including an IC card comprising a microprocessor, a read-only memory and an electronically erasable programmable read only memory, said system comprising:

means for manufacturing said IC card and for storing at the time of manufacture in said read-only memory an operating system and programming instructions; and

means for personalizing said IC card and for storing at the time of personalization in said electronically erasable programmable read only memory an address table with memory addresses of at least one of said programming instructions,

wherein the operating system will only access those program instructions in accordance with the addresses indicated in the address table.

2. The system of claim 1, wherein said programming instructions comprise at least one primitive.

3. The system of claim 1 or claim 2, wherein said programming instructions comprise at least one codelet.

4. The system of any of claims 1 to 3, wherein said means for personalizing said IC card and for storing in said electronically erasable programmable read only memory further stores additional programming instructions.

5. The system of claim 4, wherein said additional programming instructions comprise at least one primitive.

6. The system of claim 4 or claim 5, wherein said additional programming instructions comprise at least one codelet.

7. The system of claim 5 or claim 6, wherein said address table comprises a listing of the names of the primitives to be accessed and memory addresses containing the primitives.

8. The system of claim 6 wherein said address table comprises a listing of the names of the codelets to be accessed and memory addresses containing the codelets.

9. A process for providing a secure multiple application card system including an IC card comprising a microprocessor, a read-only memory and an electronically erasable programmable read only memory, said process comprising the steps of:

manufacturing said IC card and for storing at the time of manufacture in said read-only memory an operating system and programming instructions; and

personalizing said IC card after said time of manufacture by storing in said electronically erasable programmable read only memory an address table with memory addresses of at least one said programming instructions,

wherein the operating system will only access those program instructions in accordance with the addresses indicated in the address table.

10. The process of claim 9, wherein said programming instructions comprises at least one primitive.

11. The process of claim 9 or claim 10, wherein said programming instructions comprises at least one codelet.

12. The process of any of claims 9 to 11, wherein said step for storing in said electronically erasable programmable read only memory further includes storing additional programming instructions.

13. The process of claim 12, wherein said additional programming instructions comprises at least one primitive.

14. The system of claim 12 or claim 13, wherein said additional programming instructions comprises at least one codelet.

15. The system of claim 12 or claim 13, wherein said address table comprises a listing of the names of the primitives to be called and memory addresses containing the primitives.

16. The system of claim 14, wherein said address table comprises a listing of the names of the codelets to be called and memory addresses containing the codelets.

17. A process for providing a secure multiple application card comprising a microprocessor, a first memory and second memory, said process comprising the steps of:

a. storing in said first memory an operating system and programming instructions; and

b. personalizing said IC card after said storing step *a* by storing in said second memory an address table with memory addresses of at least one said programming instructions;

wherein said operating system will only access those program instructions in accordance with the address indicated in the address table.

18. The process of claim 17, wherein said programming instructions comprises at least one primitive.

19. The process of claim 17 or claim 18, wherein said programming instructions comprises at least one codelet.

20. The process of any of claims 17 to 19, wherein said step for storing in said electronically

erasable programmable read only memory further includes storing additional programming instructions.

21. The process of claim 20, wherein said additional programming instructions comprises at least one primitive.

22. The system of claim 20 or claim 21, wherein said additional programming instructions comprises at least one codelet.

23. The system of claim 21 or claim 22, wherein said address table comprises a listing of the names of the primitives to be called and memory addresses containing the primitives.

24. The system of claim 22, wherein said address table comprises a listing of the names of the codelets to be called and memory addresses containing the codelets.

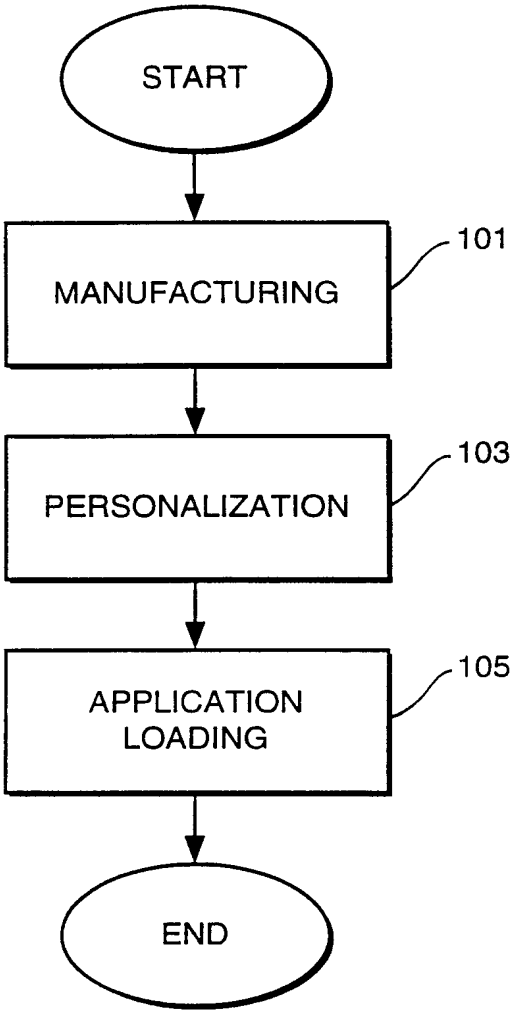

START
MANUFACTURING
101
PERSONALIZATION
103
APPLICATION LOADING
105
END

FIG.1

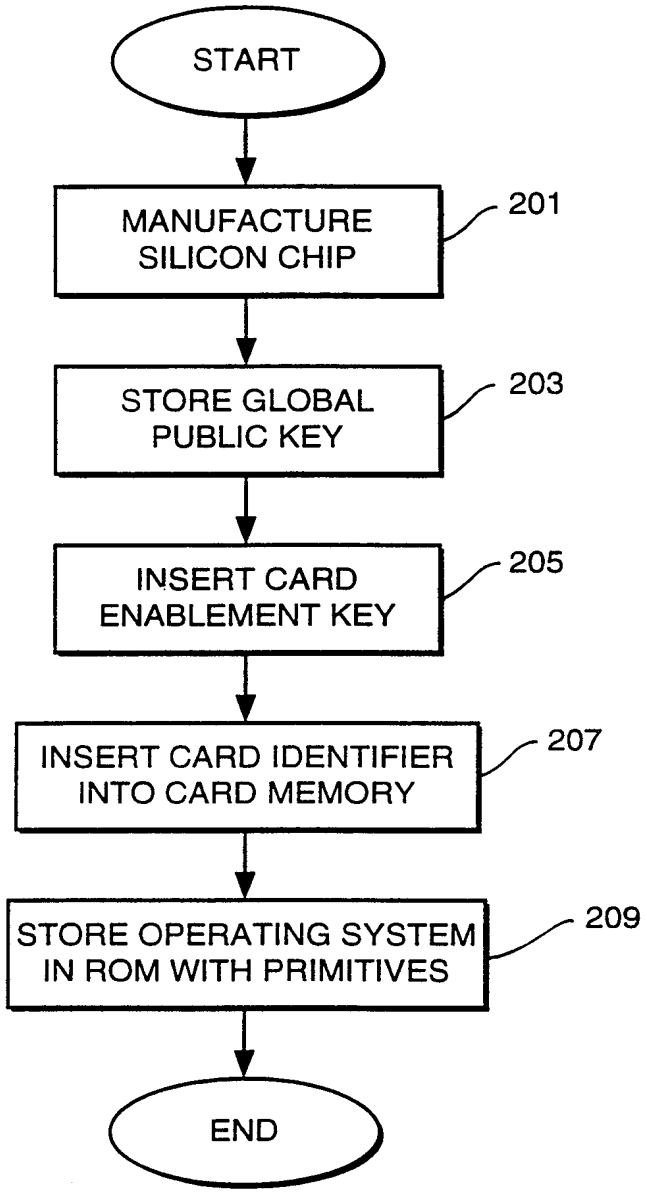

START
MANUFACTURE SILICON CHIP
201
STORE GLOBAL PUBLIC KEY
203
INSERT CARD ENABLEMENT KEY
205
INSERT CARD IDENTIFIER INTO CARD MEMORY
207
STORE OPERATING SYSTEM IN ROM WITH PRIMITIVES
209
END

FIG.2

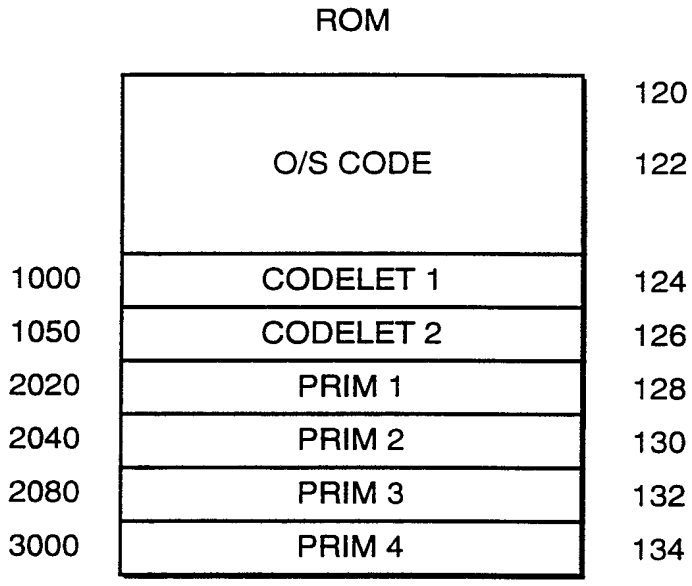

ROM
O/S CODE
120
122
1000
CODELET 1
124
1050
CODELET 2
126
2020
PRIM 1
128
2040
PRIM 2
130
2080
PRIM 3
132
3000
PRIM 4
134

FIG.3

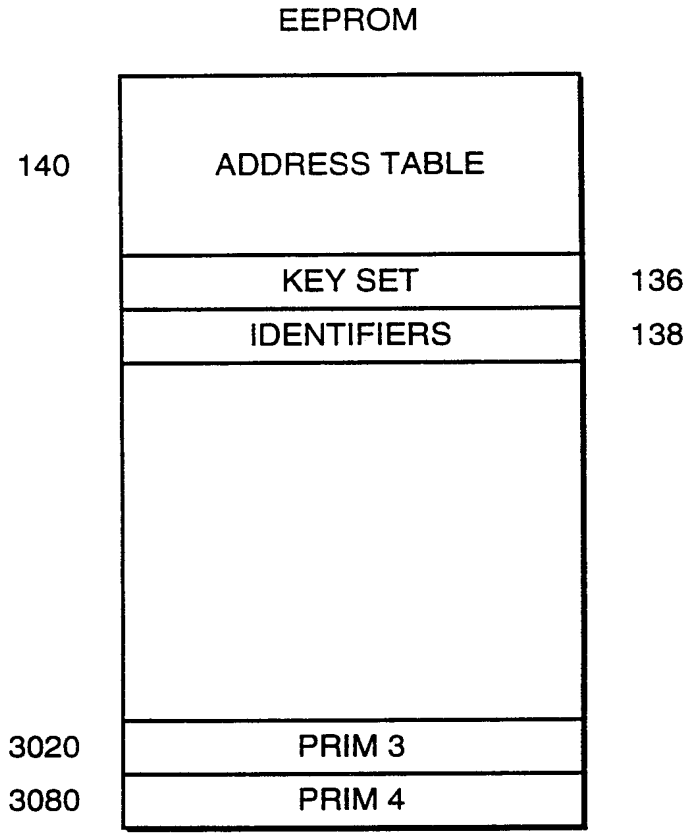



FIG.4

ADDRESS TABLE

| NAME | ADDRESS |
|---|---|
| CODELET 1 | 1000 |
| CODELET 2 | 1050 |
| PRIM 1 | 2020 |
| PRIM 2 | 2040 |
| PRIM 3 | 3020 |
| PRIM 4 | 3080 |

FIG.5

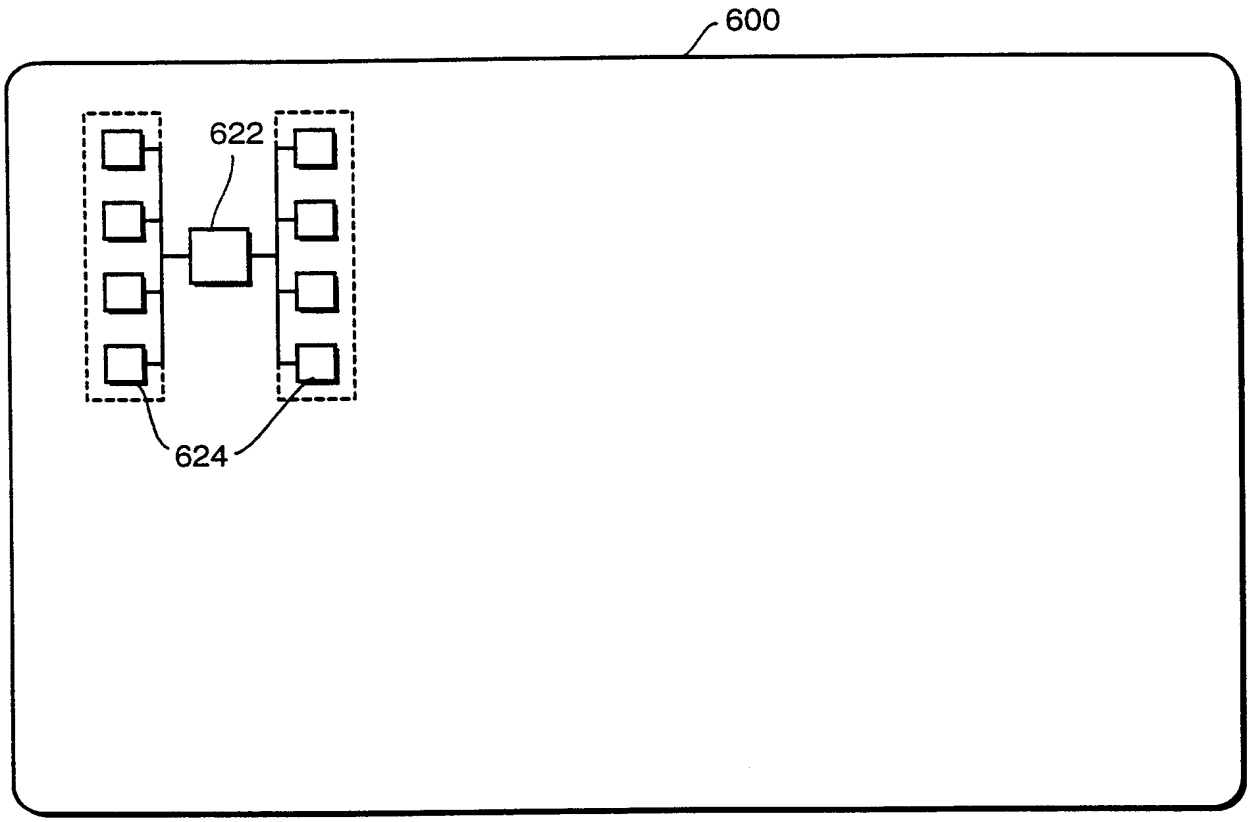

600
622
624

FIG.6

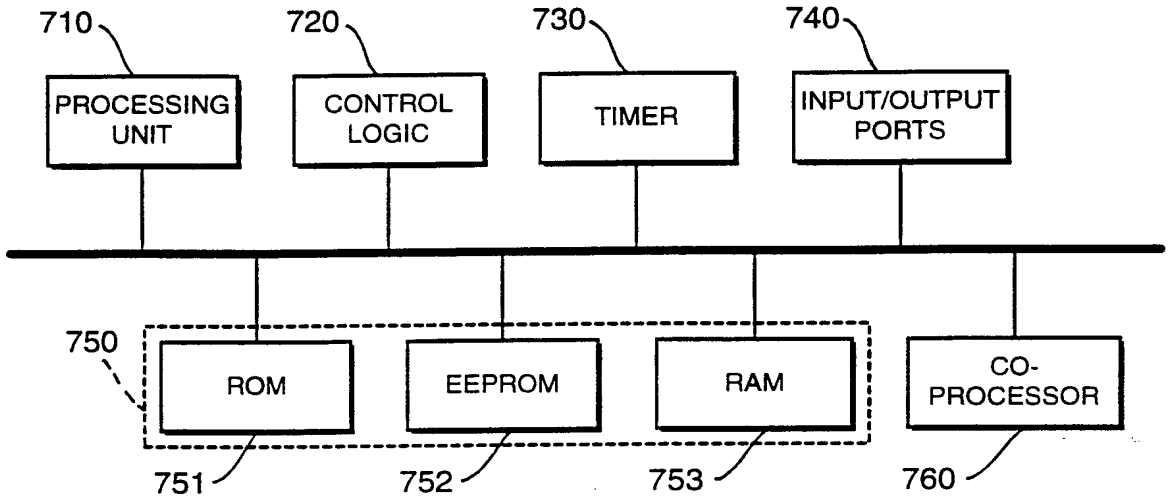

710
720
730
740
PROCESSING UNIT
CONTROL LOGIC
TIMER
INPUT/OUTPUT PORTS
750
ROM
EEPROM
RAM
CO-PROCESSOR
751
752
753
760

FIG.7

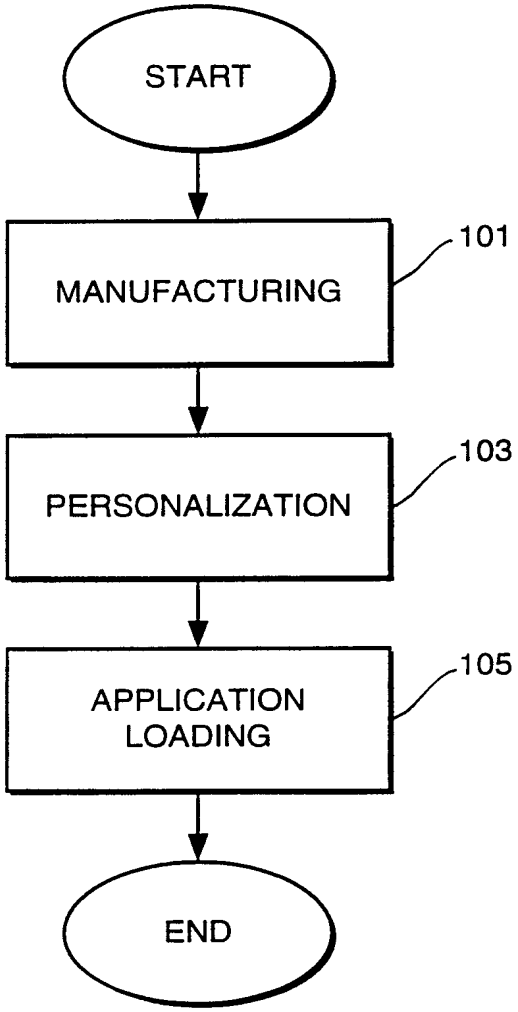



FIG.1

ANNEX A TO THE DESCRIPTION

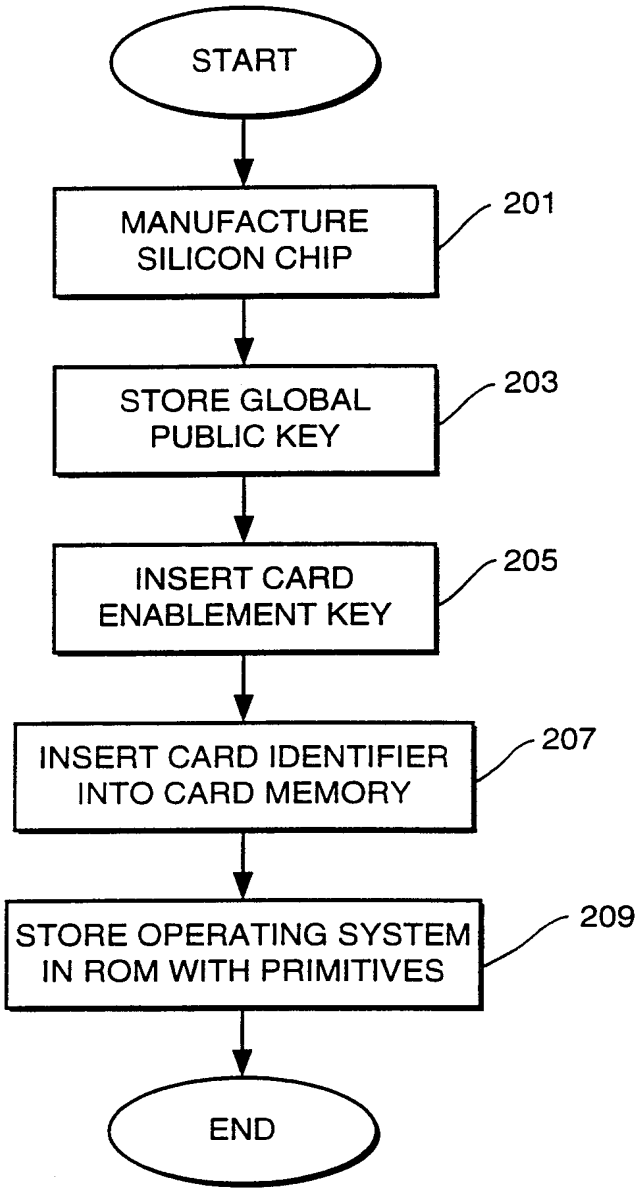



FIG.2

ANNEX A TO THE DESCRIPTION

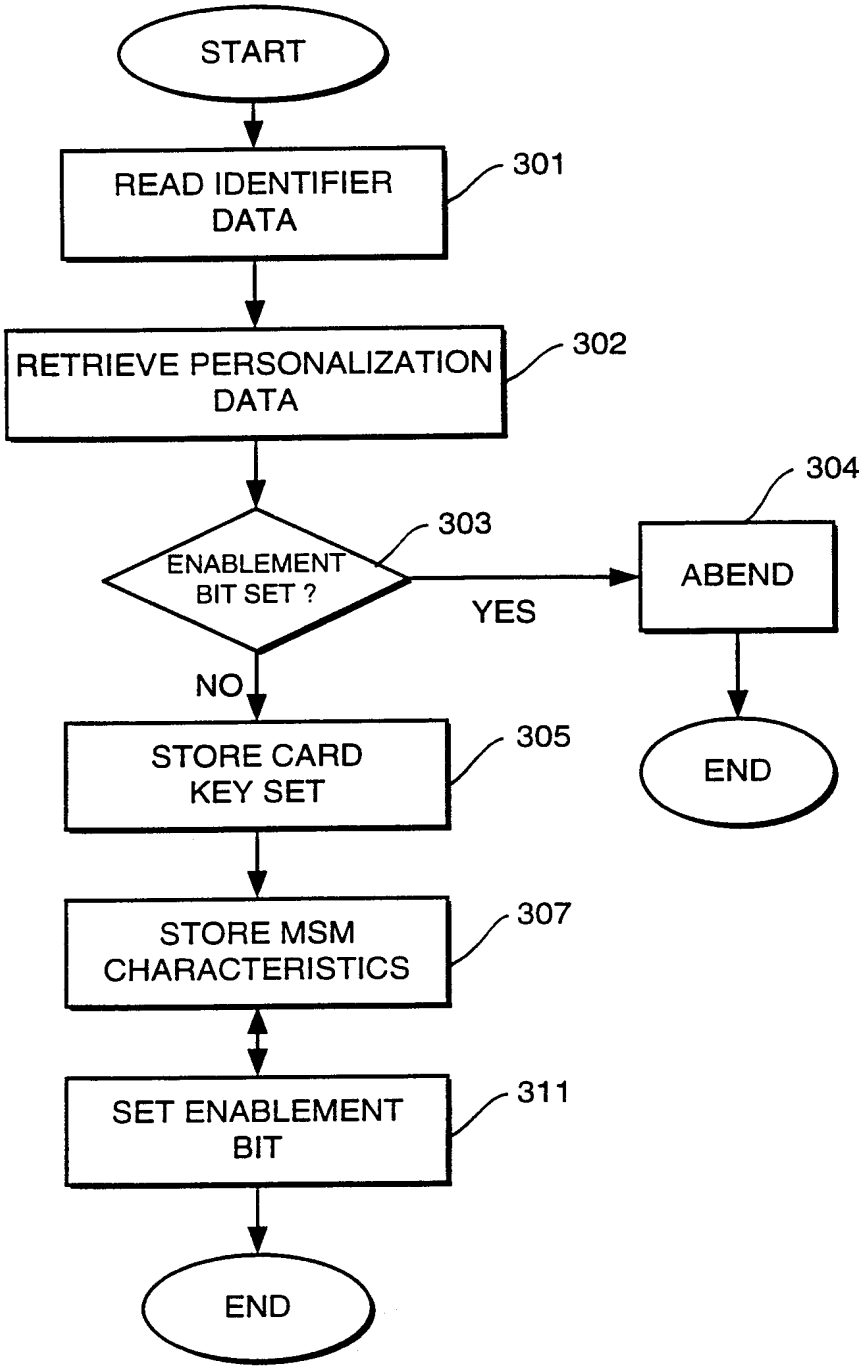



FIG.3

ANNEX A TO THE DESCRIPTION

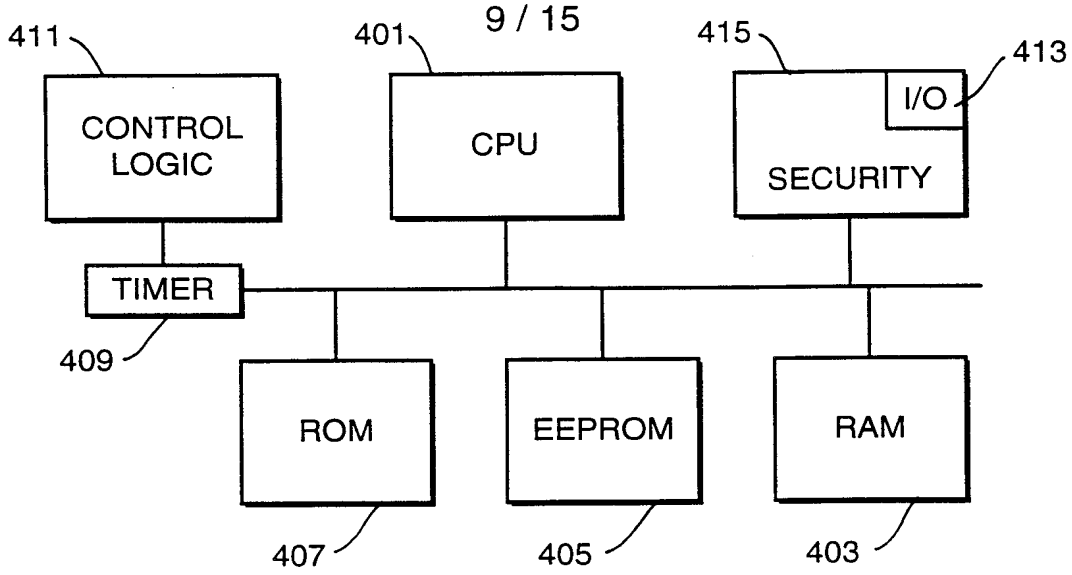



FIG.4

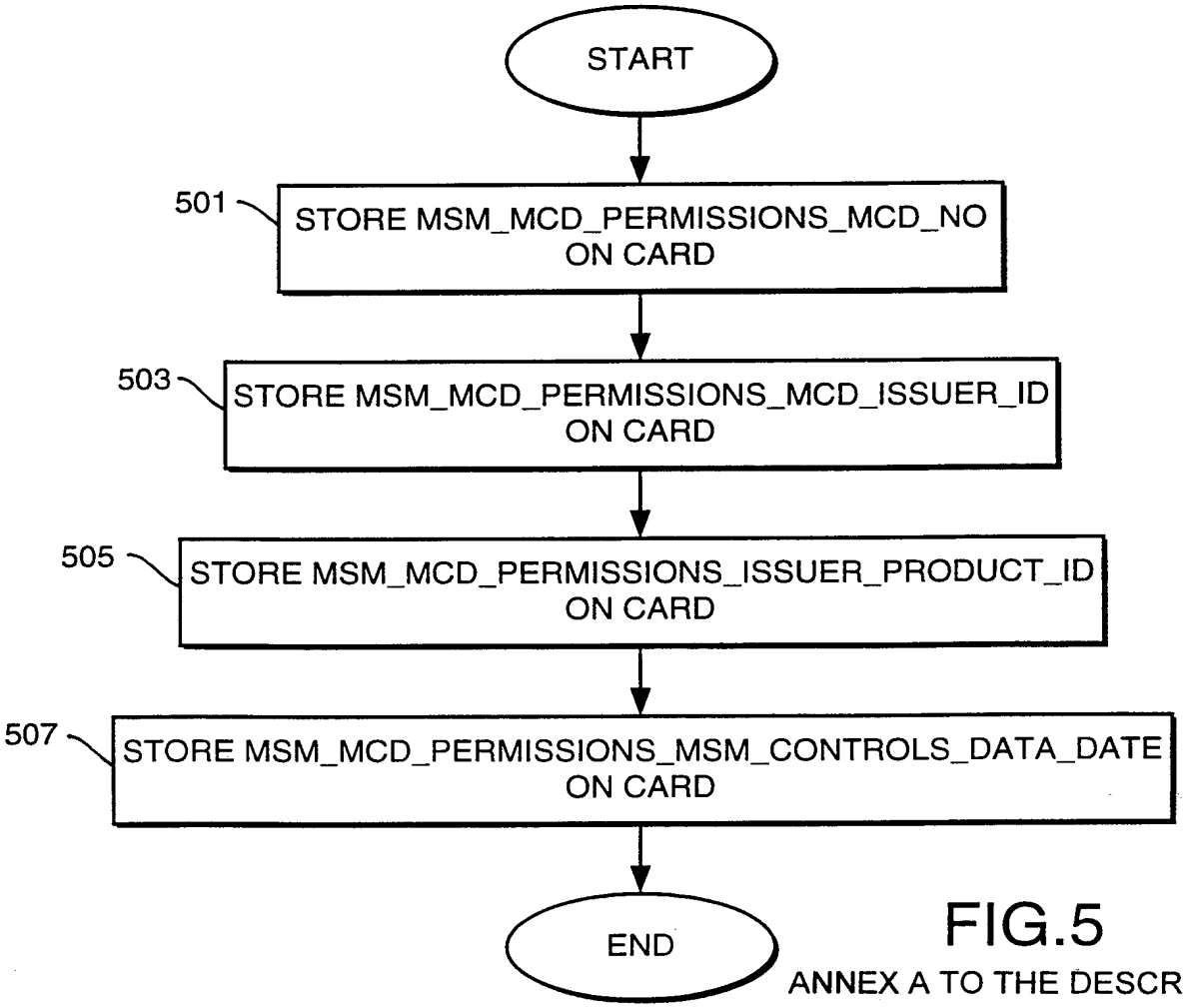



FIG.5

ANNEX A TO THE DESCRIPTION

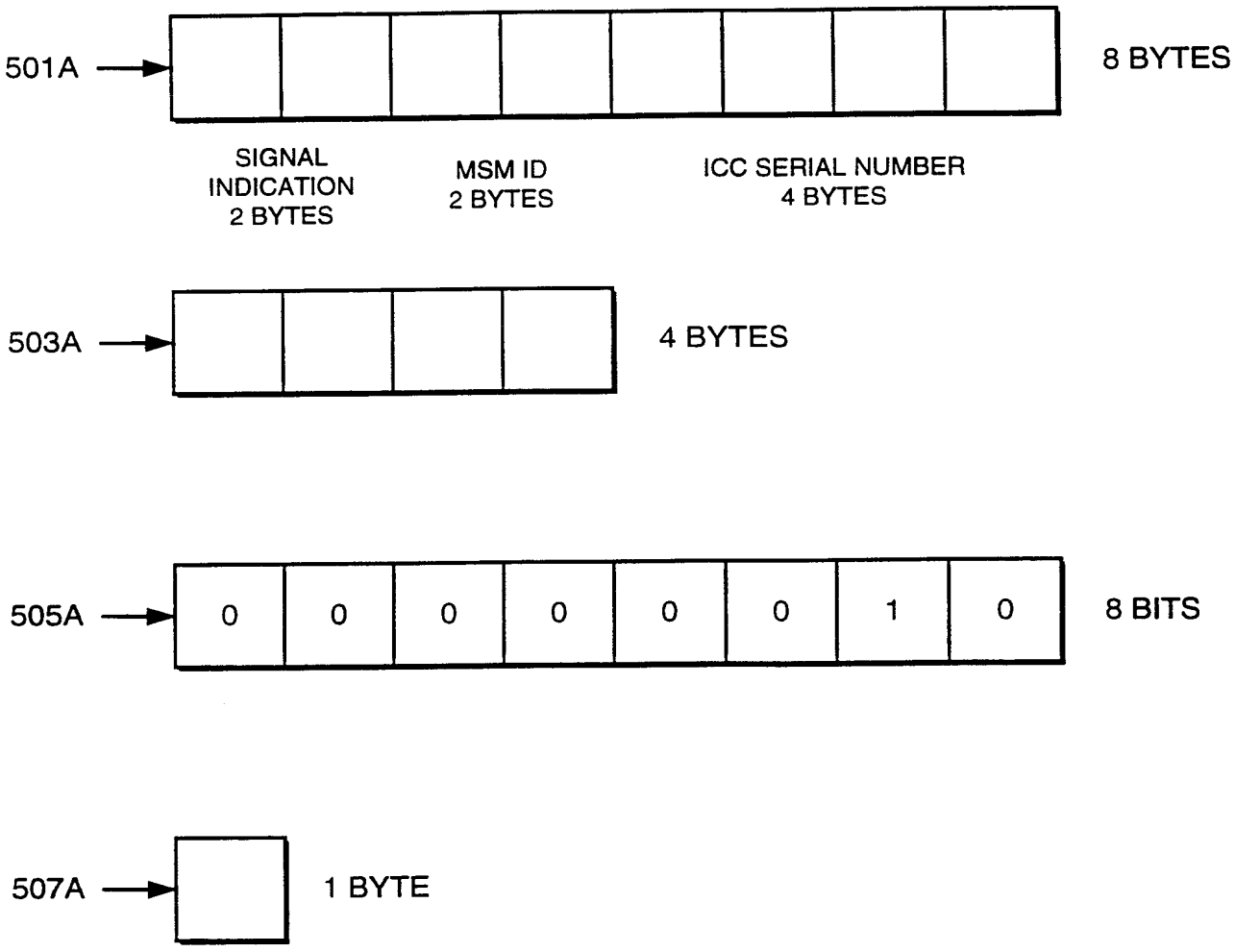



FIG.5A

ANNEX A TO THE DESCRIPTION

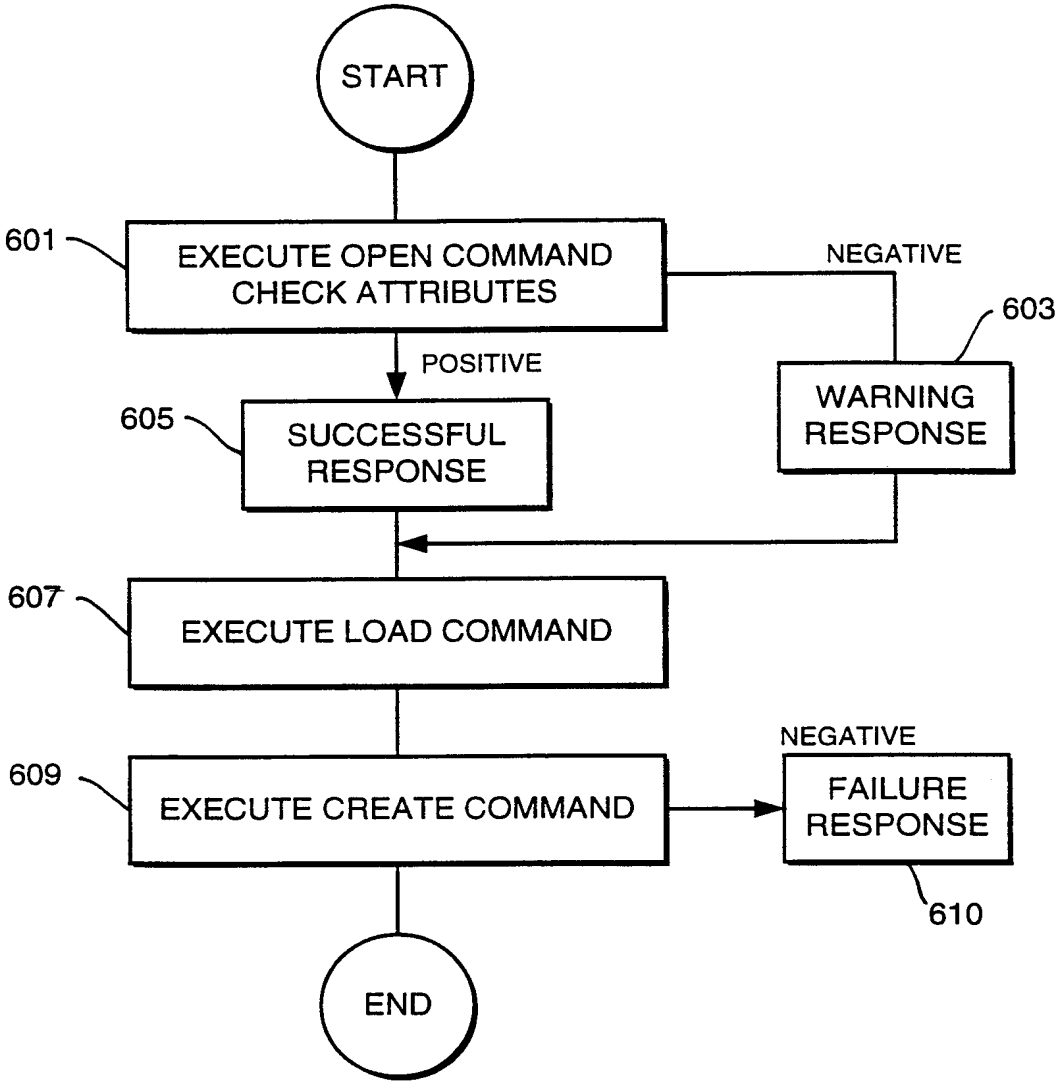



FIG.6

ANNEX A TO THE DESCRIPTION

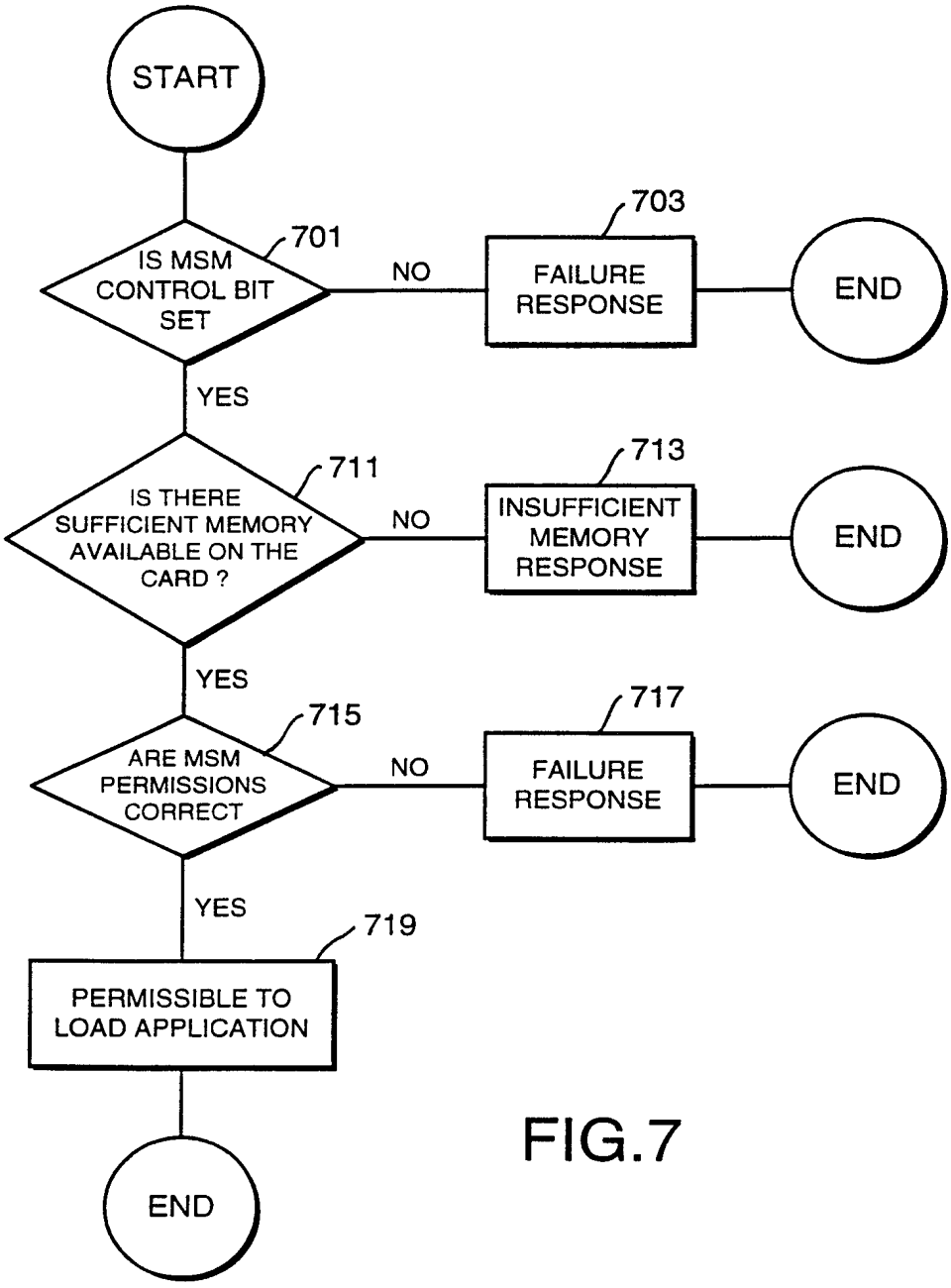



FIG.7

ANNEX A TO THE DESCRIPTION

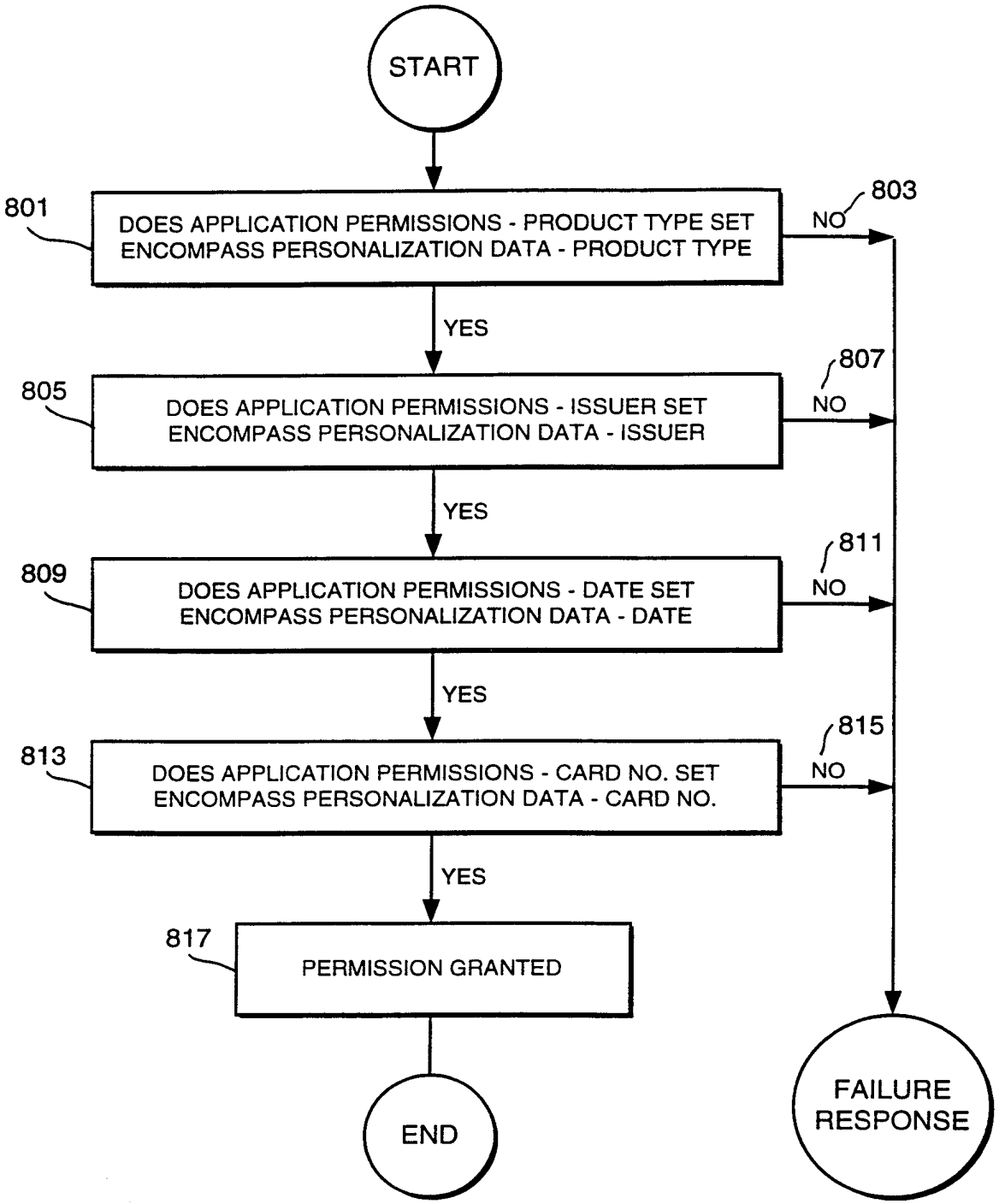



FIG.8

ANNEX A TO THE DESCRIPTION

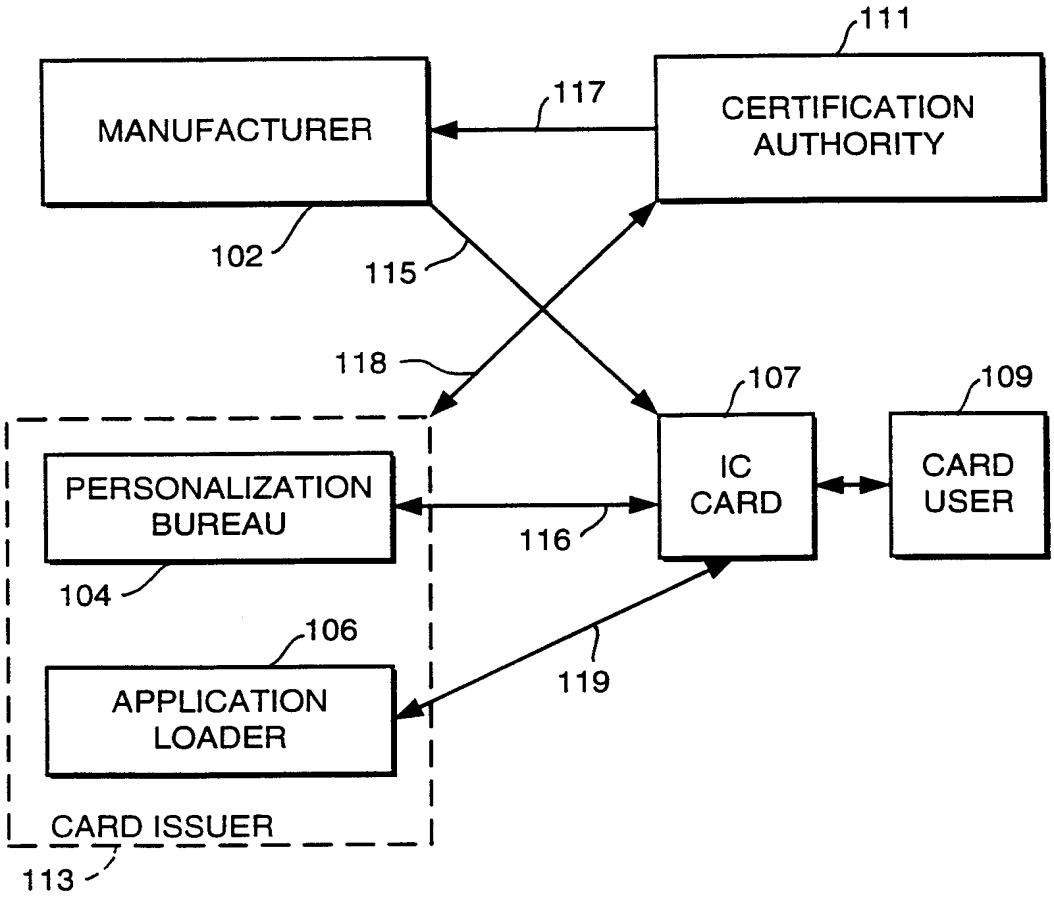



FIG.9

ANNEX A TO THE DESCRIPTION

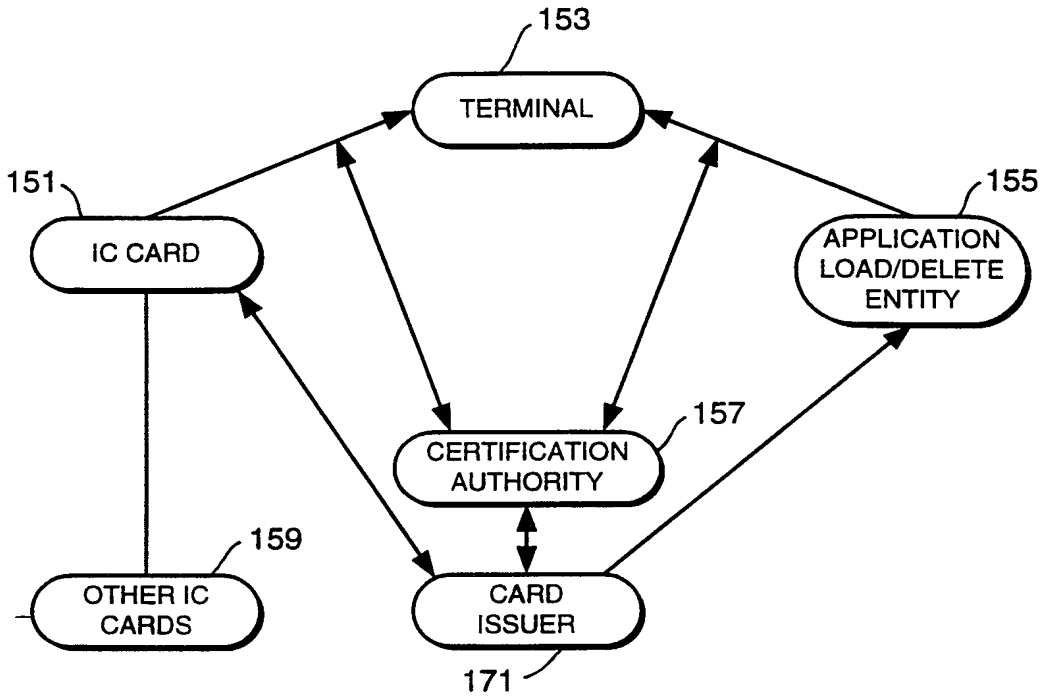



FIG.10

ANNEX A TO THE DESCRIPTION

# INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/GB 99/00289

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X<br><br>A | EP 0 218 176 A (TOSHIBA) 15 April 1987<br><br>see abstract; claims; figures<br><br>see column 3, line 42 - column 4, line 4<br>see column 6, line 31 - column 9, line 6<br>--- | 1,4,9,<br>12,17,20<br>2,3,5-8,<br>10,11,<br>13-16,<br>18,19,<br>21-24 |
| A | EP 0 466 969 A (SIEMENS NIXDORF<br>INFORMATIONSSYSTEME) 22 January 1992<br>see abstract; claims; figures<br>see column 3, line 3 - line 50<br>---<br>-/-- | 1,9,17 |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 21 June 1999 | 01/07/1999 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | David, J |

1

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/GB 99/00289

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 96 28795 A (SIEMENS) 19 September 1996<br>see the whole document | 1,4,7,9,<br>12,15,<br>17,20,23 |
| A | EP 0 451 936 A (HITACHI MAXELL)<br>16 October 1991 | |
| A | US 5 682 027 A (J.M.G. BERTINA)<br>28 October 1997 | |
| A | EP 0 190 733 A (TOSHIBA) 13 August 1986 | |

1

# INTERNATIONAL SEARCH REPORT

...formation on patent family members

Inter ...nal Application No
PCT/GB 99/00289

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 0218176 A | 15-04-1987 | JP 62269289 A | 21-11-1987 |
| | | JP 2537200 B | 25-09-1996 |
| | | JP 63006690 A | 12-01-1988 |
| | | JP 62082489 A | 15-04-1987 |
| | | DE 3682476 A | 19-12-1991 |
| | | US 4827512 A | 02-05-1989 |
| EP 0466969 A | 22-01-1992 | AT 100229 T | 15-01-1994 |
| | | DE 59004248 D | 24-02-1994 |
| | | US 5293577 A | 08-03-1994 |
| WO 9628795 A | 19-09-1996 | DE 19508724 C | 31-10-1996 |
| | | AT 170647 T | 15-09-1998 |
| | | CN 1176701 A | 18-03-1998 |
| | | DE 59600517 D | 08-10-1998 |
| | | EP 0813723 A | 29-12-1997 |
| | | ES 2120809 T | 01-11-1998 |
| | | NO 974055 A | 10-11-1997 |
| EP 0451936 A | 16-10-1991 | JP 3240127 A | 25-10-1991 |
| | | DE 69123775 D | 06-02-1997 |
| | | DE 69123775 T | 10-07-1997 |
| | | US 5252812 A | 12-10-1993 |
| US 5682027 A | 28-10-1997 | AU 687760 B | 05-03-1998 |
| | | AU 5332194 A | 24-05-1994 |
| | | WO 9410657 A | 11-05-1994 |
| | | CA 2147824 A | 11-05-1994 |
| | | EP 0706692 A | 17-04-1996 |
| | | NO 951575 A | 26-06-1995 |
| EP 0190733 A | 13-08-1986 | JP 61177585 A | 09-08-1986 |
| | | DE 3684932 A | 27-05-1992 |